数学選書 9

数学の基礎的諸分野への

現代的入門

代数概論

森田康夫著

裳華房

数学選書 9

代 数 概 論

東北大学教授
理学博士
森 田 康 夫 著

数学の基礎的諸分野への
現代的入門

東京 裳 華 房 発行

INTRODUCTION TO ALGEBRA

by

YASUO MORITA DR.SC.

SHOKABO
TOKYO

はしがき

本書は，大学の数学科における代数学の教科書として，また代数学を独習する人を対象として書かれたものである．

さて最近の数学では，位相幾何学や代数解析学に典型的に見られるように，代数学（または代数学的手法）の重要性が以前に比べ増して来ているように思う．代数学とは，数学における有用な概念を取り出し，それを抽象化し，一般化して研究をする学問である．数学が進歩し，複雑化するにつれ，このような方法がより有用となることは，ある意味では当然である．

代数学には，有限群，（代数的）整数論，代数幾何学などのように，それ自体を研究対象とするものと，ホモロジー代数や圏の理論のように，それ以外のものを研究するための手段とするものの2通りが有る．この場合，前者においては，具体的なわかりやすい結果を出すことが重要であり，後者においては，抽象的でも応用範囲の広い結果を出すことが重要である．我国においては，歴史的に前者を重視し，後者を軽視する傾向が有ったが，西洋では，抽象化や一般化にも多くの努力が払われて来たように思う．このことは日本人の国民性とも関係するが，最近の代数幾何学や，代数解析学等の発展を見ると，抽象的手法の重要性を，整数論を専門とする筆者も非常に強く感じている．

日本における代数学教育においては，群から話を始め，環，体を経て，ガロアの理論に至るコースが，歴史的に標準的なものとなっている．このことは，近代における代数学の最初のめざましい成果が，アーベルとガロアによる方程式の可解性の研究と，ガウスらによる作図可能性の研究であったこと

に由来し，その意味では，歴史に従った，妥当なカリキュラムである．しかし現在から見ると，方程式の可解性の理論や作図可能性の理論は，非常に見事な理論ではあるが，それ自体は余り重要性を持たない．むしろ最近の数学においては，ホモロジー代数を中心とした加群の理論や，圏の理論の方が，はるかに重要である．

数学教育においては，歴史にそって教育することは，自然であり，わかりやすい．しかし，現在の数学における重要性も無視すべきではない．また，群，環，体などについて詳しい結果を学ぶことも重要ではあるが，代数的な考え方を学ぶことの方がより重要である．

そこで本文では，上に述べた伝統的な代数学のカリキュラムを尊重しつつ，同時に代数的な考え方を説明することと，最近重要性を増している分野の理論を説明することにも重点を置いた．具体的には，第I章，第II章，第III章，第V章では，基礎的な概念の説明を特にていねいにするとともに，第IV章では加群のことをかなり詳しく述べた．また第VI章において，圏の理論を紹介した．

第I章では，代数学で使われる集合論の定義を思い出すと共に，演算や「群，環，加群，体」といった基礎的な概念を導入した．このため，本書を読むには，第I章をまず読むことが必要である．第II章の結果は以降で使われることが多いが，シローの定理，有限アーベル群の構造定理，べき零群，生成元と基本関係等についての結果は，以降のためには，必ずしも必要ではない．第III章の結果は，第IV章を読むためには必要だが，第V章を読むためにはネター環の理論は不要である．第IV章は，第V章を読むためには必要ではない．これらの項目のうち，通常の部分より詳しく，以後で必要でないものには，その章や節の名前に＊印を付けておいた．

代数学の教科書には，ファン・デル・ヴェルデンの本など多くの名著が有るが，本書が，読者が「代数学とは何か」を理解するための助けとなることができれば，筆者にとって望外の幸せである．

最後に，本書の執筆を勧めて戴いた東北大学の佐武一郎教授に深く感謝の意を表するとともに，本書の発行については，裳華房の細木周治氏の多くの協力があったことを記して感謝の意を表したい．

1987年11月

森田 康夫

（第2版への付記）　本書の再版にあたり，初版にあった数学的な誤りや，印刷上の誤り，さらに説明不足な点等を修正した．これについては，中央大学の百瀬文之氏，早稲田大学の橋本喜一朗氏，慶応大学の中沢英昭氏等の方に，多大な御協力を戴いた．ここに，深く感謝の意を表します．

目　次

I. 基礎概念

II. 群

III. 環

IV. 加　群*

V. 体

VI. 圏と関手*

I 基 礎 概 念

この章の前半では，集合についての記号を導入し，同値関係とツォルンの補題について簡単に解説する．この章の後半では，群，環，体などの定義を行うとともに，多項式環，行列のなす環など重要な例をあげる．

§1. 集合と写像

$\forall, \exists, \nexists, \Longrightarrow, \Longleftrightarrow$ で，それぞれ‘任意の’，‘存在する’，‘存在しない’，‘… ならば … となる’，‘… と … は同値である’，を意味する論理記号を表す．

$\emptyset$ を空集合とし，$\boldsymbol{N}$ を自然数の全体，$\boldsymbol{Z}$ を整数の全体，$\boldsymbol{Q}$ を有理数の全体，$\boldsymbol{R}$ を実数の全体，$\boldsymbol{C}$ を複素数の全体を表す記号とする．

A を集合とするとき，a が A の元であるとき $a \in A$ と書き，a が A の元でないとき $a \notin A$ と書く．

B が A の部分集合であるとき $B \subset A$ と書き，B が A の真部分集合であるとき $B \subsetneqq A$ と書く．A, B を集合とするとき，A の元で B の元ではないもの全体のなす集合を $A \setminus B$ で表す：　$A \setminus B = \{a \in A \mid a \notin B\}$．

A が部分集合 B_λ $(\lambda \in \Lambda)$ の和集合であるとき，

$$A = \bigcup_{\lambda \in \Lambda} B_\lambda$$

と表し，とくに これら B_λ が，$\lambda \neq \mu$ なら $B_\lambda \cap B_\mu = \emptyset$ を満たすとき，$A = \coprod_{\lambda \in \Lambda} B_\lambda$ と表す．

有限集合 A に対し，A の元の個数を $|A|$ または $\#A$ で表し，無限集合 A に対しては $|A| = \infty$ とおく．

$A_1, A_2, \cdots, A_n$ を集合とするとき, $a_1 \in A_1$, $a_2 \in A_2$, $\cdots$, $a_n \in A_n$ より作った順序をつけた組を $(a_1, a_2, \cdots, a_n)$ で表し，その全体を $A_1 \times A_2 \times \cdots \times A_n$ で表し，$A_1, A_2, \cdots, A_n$ の **直積** とよぶ. このとき

$$|A_1 \times A_2 \times \cdots \times A_n| = |A_1| \times |A_2| \times \cdots \times |A_n|$$

が成り立つ.

f が集合 A から集合 B への写像であるとき,

$$f:\quad A \longrightarrow B$$

と表す. また この写像により $a \in A$ に $b \in B$ が対応しているとき,

$$f:\quad A \ni a \quad \longmapsto \quad b \in B$$

などと書く.

f が A から B への写像で，$A_0 \subset A$ のとき，$f(a)$ $(a \in A_0)$ 全体のなす集合を $f(A_0)$ で表し，f による A_0 の **像** とよぶ. とくに $A_0 = A$ のとき，$f(A)$ のことを $\mathrm{Im}(f)$ と表す： $\mathrm{Im}(f) = \{f(a) \mid a \in A\}$.

$B_0 \subset B$ のとき，$f(a) \in B_0$ となる $a \in A$ 全体のなす集合を $f^{-1}(B_0)$ で表し，f による B_0 の **逆像** とよぶ： $f^{-1}(B_0) = \{a \in A \mid f(a) \in B_0\}$. とくに B_0 が 1 つの元 b から成るとき，これを $f^{-1}(b)$ で表す.

A の任意の 2 元 a_1, a_2 について

$$a_1 \neq a_2 \quad \Longrightarrow \quad f(a_1) \neq f(a_2)$$

が成り立つとき，f は **単射** または **1 対 1** であるという. また $\mathrm{Im}(f) = B$ となるとき，f は **全射** または **上への写像** であるという.

写像 f： $A \longrightarrow B$ が全射かつ単射となるとき，f は **全単射** であるという. このとき，B の任意の元 b に対し，$f(a) = b$ となる $a \in A$ は唯一つ存在し，これにより

$$f^{-1}:\quad B \ni b \quad \longmapsto \quad a = f^{-1}(b) \in A$$

なる写像ができる. これを f の **逆写像** という. f： $A \longrightarrow B$ なる全単射が存在すれば，f により A の元と B の元が 1 対 1 に対応するから，$|A| = |B|$ と

なる.

$B \subset A$ のとき, B の元 b に A の元とみての b を対応させる写像 $B \ni b \longmapsto b \in A$ を, B の A への **埋め込み** といい, $B \hookrightarrow A$ などと表す. とくに $B = A$ のとき, $A \ni a \longmapsto a \in A$ を id_A で表し, A の **恒等写像** とよぶ.

$f: A \longrightarrow B$ と $g: B \longrightarrow C$ なる2つの写像の **合成** を $g \circ f$ で表す. $g \circ f: A \longrightarrow C$ は, $a \in A$ に対し

$$(g \circ f)(a) = g(f(a))$$

で定義されている.

問題 1.1 A が有限集合のとき, 写像 $f: A \longrightarrow A$ について,

(1) 全射である, (2) 単射である, (3) 全単射である

の3つは, 互いに同値であることを示せ.

§2. 同値関係

集合 A において **関係** R が定められているとは, 直積集合 $A \times A$ の部分集合 R が定義されていることをいう. このとき, $a, b \in A$ が $(a, b) \in R$ を満たすなら aRb と書く. 集合 A における **同値関係** $\sim$ とは, この意味での関係であり, しかも 次の3条件を満たすものをいう.

(E1) 反射律: $a \sim a$,

(E2) 対称律: $a \sim b \implies b \sim a$,

(E3) 推移律: $a \sim b,\ b \sim c \implies a \sim c$.

このとき $a \sim b$ なら, a と b とは (同値関係 $\sim$ に関して) **同値** であるという. また a と同値なもの全体のなす集合を $C(a)$ で表し, a を含む **同値類** とよぶ.

同値類について,

(1) $a \in C(a)$,

(2) $b \in C(a) \implies C(b) = C(a)$

$$(3)\qquad C(a)\neq C(b)\implies C(a)\cap C(b)=\emptyset$$

が成り立つことが確かめられる.

(1) より, $A=\bigcup_{a\in A}C(a)$ となるが, 各 $C(a)$ より1つずつ a_λ を選ぶと, (2),(3) より

$$A=\coprod_{\lambda\in\Lambda}C(a_\lambda)$$

と, A が部分集合 $C(a)$ の和に分割されることがわかる. これを同値関係 $\sim$ による集合 A の **類別** という. またこのような a_λ を同値類 $C(a_\lambda)$ の **代表元** とよび, $\{a_\lambda \mid \lambda\in\Lambda\}$ を A の同値関係 $\sim$ に関する **完全代表系** という.

逆に $A=\coprod_{\lambda\in\Lambda}C_\lambda$ を, 集合 A の部分集合への分割とするとき,

$$a\sim b \iff a,b \text{ はある共通の } C_\lambda \text{ に入る}$$

とおくと, この $\sim$ は A の同値関係となり, $A=\coprod C_\lambda$ はこの同値関係による類別となる.

例 2.1　m を正の整数, $\boldsymbol{Z}$ を整数の全体とする. $a,b\in\boldsymbol{Z}$ に対して

$$a\sim b \iff a-b \text{ は } m \text{ の倍数}$$

とおく. このとき $a-b=mt$ $(t\in\boldsymbol{Z})$ と書ける. よって, この $\sim$ は (E 1) $\sim$ (E 3) を満たし, 同値関係となることがわかる. この例は, 以下で多く用いられ, 重要である.

§3. 順序集合とツォルンの補題

集合 A において関係 $\leqq$ が定められており, これが次の3条件を満たすとき, **順序集合** であるという.

(O 1)　反射律：　$a\leqq a$,

(O 2)　反対称律：　$a\leqq b,\quad b\leqq a\implies a=b$,

(O 3)　推移律：　$a\leqq b,\quad b\leqq c\implies a\leqq c$.

$a\leqq b$ かつ $a\neq b$ のとき $a<b$ と書く.

順序集合 A において, 常に $a\leqq b$ または $b\leqq a$ が成り立つとき, A は **全順序集合** という.

例 3. 1　Xを集合，$\mathfrak{P}(X)$ を X の部分集合全体のなす集合とする．このとき，$A, B \in \mathfrak{P}(X)$ について，

$$A \leqq B \iff A, B \text{ を } X \text{ の部分集合とみて } A \subset B$$

と定めると，これにより $\mathfrak{P}(X)$ 上の順序 $\leqq$ が定まる．これを，X の部分集合全体のなす集合上での **包含関係による順序** とよぶ．この順序は，$|X| \geqq 2$ なら全順序ではない．

順序集合 A の元 a は，$a < b$ なる元 $b \in A$ が存在しないとき **極大元** であるという．また A の元 a は，すべての $b \in A$ に対して $b \leqq a$ が成り立つとき **最大元** であるという．**極小元** と **最小元** も同様にして定義される．最大元は極大元であるが，極大元が最大元となるとは限らない．

B を順序集合 A の部分集合とする．このとき $a \in A$ がすべての B の元 b に対し $b \leqq a$ を満たすなら，a は B の **上界** であるという．また B の上界が存在するとき，B は **上に有界** であるという．順序集合 A は，$A \neq \emptyset$ であり，かつ任意の空でない全順序部分集合 B が A 内に上界をもつとき，**帰納的** であるという．

例 3. 2　$\boldsymbol{N}$ を自然数の全体とし，$a, b \in \boldsymbol{N}$ に対し

$$a \leqq b \iff a - b \text{ が負でない整数}$$

として，通常の逆向きの順序を入れる．このとき $\boldsymbol{N}$ は帰納的全順序集合となる．これに対し，正の実数の全体に同様にして順序を入れると，帰納的にはならない．

例 3. 3　例 3.1 の順序集合 $\mathfrak{P}(X)$ を考える．$\{A_\lambda\}_{\lambda \in \Lambda}$ を $\mathfrak{P}(X)$ の全順序部分集合とする．このとき $\bigcup_{\lambda \in \Lambda} A_\lambda$ は任意の A_λ を含むから，$\{A_\lambda\}_{\lambda \in \Lambda}$ の上界となる．よって $\mathfrak{P}(X)$ は帰納的順序集合となる．この例は以下たびたび使われる．

次の定理は，**ツォルンの補題** とよばれ，無限集合を扱うときの基本的手段の1つである．

定理 3. 4　帰納的順序集合には，極大元が少なくとも1つ存在する．

全順序集合 A において，任意の空でない A の部分集合が最小元をもつとき，

A は**整列集合**であるという．自然数の全体 $\boldsymbol{N}$ や，$\boldsymbol{N} \cup \{0\}$，$\boldsymbol{N} \cup \{0\} \cup \{\infty\}$ などは通常の順序で整列集合となる．

§4. 演　算

集合 A が与えられたとき，直積 $A \times A$ から A への写像 $f: A \times A \longrightarrow A$ を A の（2項）**演算**とよぶ．このとき $f(a, b)$ のことを $a \cdot b$ と書いたり，ab と書いたりする．2項演算が与えられたとき，集合 A に**乗法**が定まったといい，$a \cdot b$ のことを a, b の**積**とよぶ．

A の乗法が与えられたとき，任意の $a, b \in A$ に対し

$$a \cdot (b \cdot c) = (a \cdot b) \cdot c$$

が成り立つなら，この乗法は**結合法則**を満たすという．

例 4. 1　$A = \{a_1, a_2, \cdots, a_n\}$ 上に乗法が定まっているとする．このとき，左下の表のような正方形の表の a_i と a_j の交わるところに $a_i \cdot a_j$ を書いたものを**乗積表**という．例えば，右下の表は後にでてくる対称群 S_3 の乗積表であり，結合法則の成り立っていることが確かめられる．

	a_1	……	a_i	……	a_n
a_1			⋮		
⋮			⋮		
a_j	………		$a_i \cdot a_j$	………	
⋮			⋮		
a_n					

	1	a	b	u	v	w
1	1	a	b	u	v	w
a	a	b	1	v	w	u
b	b	1	a	w	u	v
u	u	w	v	1	b	a
v	v	u	w	a	1	b
w	w	v	u	b	a	1

A の乗法が与えられたとき，

$$a \cdot b = b \cdot a$$

が常に成り立つとき，この乗法は**可換**であるといい，**交換法則**が成り立つという．この場合，この演算を $a + b$ の形で書き，**加法**とよぶことがある．

A の乗法 $a\cdot b$ と加法 $a+b$ が与えられたとき，

$$a\cdot(b+c)=a\cdot b+a\cdot c$$

$$(a+b)\cdot c=a\cdot c+b\cdot c$$

の 2 つが常に成り立つなら，**分配法則** が成り立つという．

演算の定義を，$f:\ A_1\times A_2\longrightarrow A_3$ なる写像として一般化すると便利なことがある．とくに $A_2=A_3=B,\ A_1=A$ なる場合が良く使われる．A にも B にも結合法則を満たす乗法が定まっており，$f:\ A\times B\longrightarrow B$ の演算が与えられたとする．この演算に関する積も $a\cdot b\ (a\in A,\ b\in B)$ で表すとき，結合法則と類似の法則

$$(a_1\cdot a_2)\cdot b=a_1\cdot(a_2\cdot b)\qquad (a_1,a_2\in A,\ b\in B)$$

が成り立つなら，A の B への **作用** が定まったという．

例 4. 2　A を 2×2 型の実正方行列の全体 $M_2(\boldsymbol{R})$ とし，A での行列の和を $a+b$，A での行列の積を $a\cdot b$ で表す．また $\lambda\in\boldsymbol{R}$ に対し，a の λ 倍を $\lambda\cdot a$ で表し，

$$[a,b]=a\cdot b-b\cdot a$$

とおく．このとき，A の演算 $+$ と $\cdot$ については結合法則が成り立つが，[,] については結合法則が成り立たない．また $+$ については交換法則が成り立つが，$\cdot$ と [,] については交換法則は成り立たない．$+$ と $\cdot$，および $+$ と [,] の組に対しては分配法則が成り立つ．さらに $\boldsymbol{R}\times A\ni(\lambda,a)\longmapsto\lambda\cdot a\in A$ なる演算は，$(\lambda_1\cdot\lambda_2)\cdot a=\lambda_1\cdot(\lambda_2\cdot a)$ を満たし，作用となっている．

集合 A において演算 $A\times A\longrightarrow A$ が定義されており，この演算が結合法則

$$(a\cdot b)\cdot c=a\cdot(b\cdot c)$$

を満たすとき，A は **半群** であるという．半群 A においては，

$$(a_1\cdot a_2)\cdot(a_3\cdot a_4)=a_1\cdot((a_2\cdot a_3)\cdot a_4)=(a_1\cdot(a_2\cdot a_3))\cdot a_4$$

などのように，n 個の元 $a_1,a_2,\cdots,a_n$ の積は，演算を行う順序（括弧のつけ方）によらずに一意的に定まる．これを **一般化された結合法則** とよぶ．この

意味で，$a_1, a_2, \cdots, a_n$ の（この順序での）積を $a_1 \cdot a_2 \cdot \cdots \cdot a_n$ などと書く．

問題4．3　n に関する帰納法で，一般化された結合法則を証明せよ．

半群 A の元 e が，任意の $a \in A$ に対し

$$e \cdot a = a \cdot e = a$$

を満たすとき，e は A の **単位元** であるという．e' も A の単位元だとすると，

$$e' \cdot b = b \cdot e' = b$$

が任意の $b \in A$ に対して成り立つ．よって $a = e'$，$b = e$ とおくと

$$e = e \cdot e' = e'$$

が成り立つ．したがって，半群 A の単位元は，存在するとしても唯一つである．以下単位元を 1 で表す．

A を単位元 1 をもつ半群とし，a を A の元とする．このとき，$b \in A$ が

$$a \cdot b = b \cdot a = 1$$

を満たすなら，b は a の **逆元** であるという．b' も a の逆元だとすると，$a \cdot b' = b' \cdot a = 1$ が成り立つから

$$b' = b' \cdot 1 = b' \cdot (a \cdot b) = (b' \cdot a) \cdot b = 1 \cdot b = b$$

となる．よって a の逆元は存在するとしても唯一つである．a の逆元を以下 a^{-1} で表す．また逆元をもつ半群の元のことを，**正則元** または **単元** という．

半群 A において交換法則

$$a \cdot b = b \cdot a$$

が成り立つとき，A を **可換半群** であるという．このとき，A での n 個の元の積は 並べる順によらずに一定になる．

§5．群

集合 G において乗法が定まっており，この乗法に関して以下の 3 つのことが成り立つとき，G は **群** であるという．

(G 1) 結合法則： $(a \cdot b) \cdot c = a \cdot (b \cdot c)$.

(G 2) 単位元の存在： Gの元1で，任意の$a \in G$に対し，$a \cdot 1 = 1 \cdot a = a$となるものが存在する.

(G 3) 逆元の存在： Gの任意の元aに対し，Gの元a^{-1}で，$a \cdot a^{-1} = a^{-1}a = 1$となるものが存在する.

つまり，単位元と逆元の存在する半群を群という.

群Gにおいて，(G 1) ～ (G 3) の他に

(G 4) 交換法則： $a \cdot b = b \cdot a$

の成り立つものを，**アーベル群** または **可換群** という．この場合Gの演算を・の代りに＋で表すことが多い.

Gを群，a, b, x, yをGの元とする．このときa^{-1}を左から掛けることにより，

$$a \cdot x = a \cdot y \implies x = y$$

が成り立つことがわかる．同様に

$$x \cdot b = y \cdot b \implies x = y$$

も成り立つ．これらを **簡約法則** という.

また，aまたはa^{-1}を左から掛けることにより，

$$a \cdot x = b \iff x = a^{-1} \cdot b$$

が成り立つことがわかる．同様に

$$y \cdot a = b \iff y = b \cdot a^{-1}$$

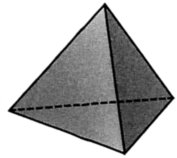
も成り立つ．つまり群では **除法** が一意的に可能である.

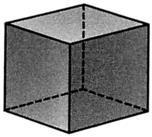
問題5.1 半群Gにおいて，除法が一意的に可能なら，Gは群となることを示せ.

問題5.2 群Gにおいては，ι： $G \ni x \longmapsto x^{-1} \in G$，$l_a$： $G \ni x \longmapsto a \cdot x \in G$ $(a \in G)$，r_a： $G \ni x \longmapsto x \cdot a \in G$ $(a \in G)$ らは全単射となることを示せ.

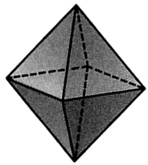
例5.3 次ページの図のような合同な正三角形4枚によって囲まれる正四面体を考える． この正四面体の重心を中心とする回転で，この正四面体をそれ自身にうつすもの全

体は，(12 個の元から成る)群を成す．これを **正四面体群** とよぶ．同様にして **正六面体群，正八面体群，正十二面体群，正二十面体群** などが作られる．

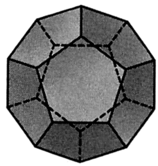




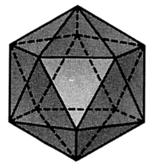
正六面体



正八面体



正十二面体



正二十面体

例 5. 4　$\boldsymbol{R}$ を実数の全体とする．$\boldsymbol{R}$ の加法と乗法は結合法則を満たす．$\boldsymbol{R}$ の加法については 0 が単位元となり，$a \in \boldsymbol{R}$ の逆元は $-a$ が与えるから，$\boldsymbol{R}$ は加法群をなす．$\boldsymbol{R}$ の乗法については，1 が単位元となり，0 以外の $a \in \boldsymbol{R}$ については逆元 a^{-1} が存在する．しかし，0 の乗法に関する逆元は存在せず，$\boldsymbol{R}$ は乗法に関しては群とならない．以上は，$\boldsymbol{R}$ を複素数の全体 $\boldsymbol{C}$ や有理数の全体 $\boldsymbol{Q}$ でおき換えても成り立つ．

例 5. 5　2×2 型の実正方行列の全体 $M_2(\boldsymbol{R})$ は，行列の和に関してアーベル群をなす．$M_2(\boldsymbol{R})$ は，行列の積に関しては単位行列 E_2 を単位元とする半群をなすが，群にはならない．一般に M が単位元をもつ半群のとき，その正則元の全体 $U(M)$ は群をなす．いまの場合，$U(M_2(\boldsymbol{R}))$ は，行列式が 0 でない正方行列の全体 $GL_2(\boldsymbol{R})$ と一致する．

例 5. 6　集合 X に対して，

$$S(X) = \{\sigma :\ X \to X \mid \text{全単射}\}$$

とおく．このとき $S(X)$ は写像の合成に関して群をなす．$S(X)$ を X 上の **置換群** とよぶ．

とくに X が集合 $\{1, 2, \cdots, n\}$ のとき，$S(X)$ を S_n で表し，n 次の **対称群** とよぶ．S_n の元 σ は，σ による $1, 2, \cdots, n$ の行き先 $\sigma(1), \sigma(2), \cdots, \sigma(n)$ を指定すると定まるから，

$$\sigma = \begin{pmatrix} 1, & 2, & \cdots, & n \\ \sigma(1), & \sigma(2), & \cdots, & \sigma(n) \end{pmatrix}$$

とも書く．

$\varDelta(x_1, x_2, \cdots, x_n)$ を $x_1, x_2, \cdots, x_n$ の多項式

$$\Delta(x_1, x_2, \cdots, x_n) = \prod_{i,j} (x_i - x_j) \qquad \begin{pmatrix} (i,j) \text{ は } 1 \leqq j < i \leqq n \\ \text{を満たす組全体を動く} \end{pmatrix}$$

とする．ここで，右辺の積において i, j を $\sigma(i), \sigma(j)$ でおき換えた積を

$$\Delta_\sigma(x_1, x_2, \cdots, x_n) = \prod_{i,j} (x_{\sigma(i)} - x_{\sigma(j)})$$

で表す．このとき $\sigma(i), \sigma(j)$ は，$1 \leqq \sigma(i), \sigma(j) \leqq n$，$\{\sigma(1), \sigma(2), \cdots, \sigma(n)\} = \{1, 2, \cdots, n\}$ なる条件を満たすから，$\Delta_\sigma(x_1, x_2, \cdots, x_n)$ は $\Delta(x_1, x_2, \cdots, x_n)$ と符号を除いて一致する．そこで

$$\Delta_\sigma(x_1, x_2, \cdots, x_n) = \mathrm{sgn}(\sigma)\ \Delta(x_1, x_2, \cdots, x_n)$$

により，σ の **符号** $\mathrm{sgn}(\sigma) = \pm 1$ を定義する．

この符号 $\mathrm{sgn}(\sigma)$ が 1 のとき，σ は **偶置換** であるといい，$\mathrm{sgn}(\sigma)$ が -1 のとき σ は **奇置換** であるという．

σ が i と j $(1 \leqq i, j \leqq n,\ i \neq j)$ を入れ替え，その他の元を動かさないとき，σ は i と j の **互換** であるという．互換は奇置換である．一般に，対称群 S_n の任意の元 σ は，有限個の互換の積として表されることを第Ⅱ章，§3 で示す．これを使うと，σ が m 個の互換の積として表されるとき，$\mathrm{sgn}(\sigma) = (-1)^m$ となるといえる．このことは，後に行列式を定義するのに使われる．

§6. 環 と 体

集合 R 上に 2 つの演算 $+$ と $\cdot$ が定義されており，これらが次の 4 条件を満たすとき，R は（単位元 1 をもつ）**環** であるという．

(R 1) R は和 $+$ に関しアーベル群をなす．

(R 2) R は積 $\cdot$ に関し半群をなす．

(R 3) R は $+$ と $\cdot$ の組に関し，分配法則

$$a \cdot (b + c) = a \cdot b + a \cdot c, \qquad (a + b) \cdot c = a \cdot c + b \cdot c$$

を満たす．

(R 4) 単位元の存在： R の加法に関する単位元を 0 で表すとき，0 とは異なる R の元 1 で，乗法に関する単位元となるものが存在する．

この 1 を R の **単位元** とよび，0 を **零元** とよぶ．

R が (**R 1**) ～ (**R 4**) の他に

(**R 5**)　交換法則：　　　$a \cdot b = b \cdot a$

を満たすとき，R は **可換環** であるという．

環 R の零元 0 は，R の任意の元 x に対し　$0 \cdot x = (0+0) \cdot x = 0 \cdot x + 0 \cdot x$，$x \cdot 0 = x \cdot (0+0) = x \cdot 0 + x \cdot 0$　を満たすから，

$$0 \cdot x = x \cdot 0 = 0$$

を満たす．したがって，$0 \neq 1$ に注意すると，環の零元 0 は乗法・に関する逆元をもたないことがわかる．R の乗法に関する 正則元全体の集合を $U(R)$ または R^* で表し，R の **単数群** とよぶ．また $U(R)$ の元を R の **単数** とよぶ．

環 R において，0 以外の任意の元が乗法に関して逆元をもつとき，R は **斜体** であるという．とくに，可換環である斜体を **体** または **可換体** とよぶ．

例 6．1　整数の全体 $\boldsymbol{Z}$ は可換環をなし，有理数の全体 $\boldsymbol{Q}$，実数の全体 $\boldsymbol{R}$，複素数の全体 $\boldsymbol{C}$ などは体をなす．また，2×2 型実正方行列の全体 $M_2(\boldsymbol{R})$ は，行列の和と行列の積に関し（可換でない）環をなす．

環 R の元 a が，0 でない R の元 b に対し $a \cdot b = 0$ となるとき，a は R の **左零因子** であるという．**右零因子** も同様に定義され，双方をあわせ **零因子** とよぶ．a の逆元 a^{-1} が存在すれば，$a \cdot b = 0$ より $b = (a^{-1} \cdot a) \cdot b = a^{-1} \cdot (a \cdot b) = 0$ となるから，R の単数は零因子とはならない．したがって，斜体は 0 以外の零因子をもたないことがわかる．

R が可換環のときは，$a \cdot b = b \cdot a$ となるから，左零因子と右零因子は一致し，単に零因子とよばれる．0 は零因子であるが，それ以外に零因子をもたない可換環を **整域** とよぶ．

例 6．2　$m \geqq 2$ を整数とし，整数の全体 $\boldsymbol{Z}$ に同値関係 ～ を

$$a \sim b \iff a - b \in m\boldsymbol{Z} = \{ma \mid a \in \boldsymbol{Z}\}$$

で定め，$a \sim b$ のとき $a \equiv b \pmod{m}$ と表す．$a \equiv b \pmod{m}$ の成り立たぬとき $a \not\equiv b \pmod{m}$ と表す．$\boldsymbol{Z}$ をこの同値関係で類別した集合を $\boldsymbol{Z}/m\boldsymbol{Z}$ で表し，$a \in \boldsymbol{Z}$ を含む

類を $a \pmod m$ で表す．この同値関係に関して $\{0, 1, 2, \cdots, m-1\}$ は完全代表系をなす．

$$a \equiv c \pmod m, \qquad b \equiv d \pmod m$$

なら

$$a+b \equiv c+d \pmod m, \qquad a \cdot b \equiv c \cdot d \pmod m$$

が成り立つから，$\boldsymbol{Z}$ における和 $+$ と積・は，$\boldsymbol{Z}/m\boldsymbol{Z}$ における和 $\{a \pmod m\} + \{b \pmod m\} = a+b \pmod m$ と積 $\{a \pmod m\} \cdot \{b \pmod m\} = a \cdot b \pmod m$ を定めていることがわかる．$\boldsymbol{Z}$ においては，結合法則，分配法則などが成り立つから，$\boldsymbol{Z}/m\boldsymbol{Z}$ においても結合法則，分配法則などが成り立つ．また $m \geqq 2$ と仮定したから，$1 \not\equiv 0 \pmod m$ も成り立ち，これにより $\boldsymbol{Z}/m\boldsymbol{Z}$ が可換環となることがわかる．

$m = p_1^{e_1} p_2^{e_2} \cdots p_t^{e_t}$ (p_i は素数，$e_i \in \boldsymbol{N}$) を m の素因数分解とする．$t \geqq 2$ なら $a \equiv p_1^{e_1} \pmod m$, $b \equiv p_2^{e_2} p_3^{e_3} \cdots p_t^{e_t} \pmod m$ とおくと

$$a \not\equiv 0 \pmod m, \qquad b \not\equiv 0 \pmod m, \qquad a \cdot b \equiv 0 \pmod m$$

となるから，$\boldsymbol{Z}/m\boldsymbol{Z}$ は零因子をもつ．$t=1$, $e_1 \geqq 2$ なら $a \equiv p_1 \pmod m$, $b \equiv p_1^{e_1-1} \pmod m$ とおくと，これらも上と同じ条件を満たし，$\boldsymbol{Z}/m\boldsymbol{Z}$ が零因子をもつことがわかる．

m が素数 p であったとする．このとき，$\boldsymbol{Z}/p\boldsymbol{Z}$ の元 $a \pmod p$ が 0 でないとは，a が p で割れないことを意味する．したがって，$a \not\equiv 0 \pmod p$ なら，a と p は互いに素となるから，$cp + da = 1$ を満たす $c, d \in \boldsymbol{Z}$ が存在する．このとき

$$d \cdot a \equiv 1 \pmod p$$

となるから，$a \pmod p$ は乗法に関する逆元 $d \pmod p$ をもつ．よって $\boldsymbol{Z}/p\boldsymbol{Z}$ は体となる．

§7. 加　群

R を環とし，M を加法 $+$ の定義されたアーベル群とする．R と M との演算 $R \times M \longrightarrow M$ が定義されており，この演算に関する $r \in R$ と $m \in M$ の積 $r \cdot m$ が次の条件を満たすとき，M を**左 R-加群**であるという．

(**M 1**)　　$r \cdot (m + m') = r \cdot m + r \cdot m'$,

(**M 2**)　　$(r + r') \cdot m = r \cdot m + r' \cdot m$,

(**M 3**)　　$(r\cdot r')\cdot m = r\cdot(r'\cdot m)$,

(**M 4**)　　$1\cdot m = m$.

(**M 1**), (**M 2**) は分配法則, (**M 3**) は結合法則の類似と思え, (**M 4**) は R の単位元が M の上に恒等写像として作用することを意味する.

右 R–加群 も, 左 R–加群と同様にして定義される. R, S が環で, M が左 R–加群かつ右 S–加群であるとする. このとき

$$(r\cdot m)\cdot s = r\cdot(m\cdot s) \qquad (r\in R,\ s\in S,\ m\in M)$$

が成り立つなら, M は (R, S)–**両側加群** であるという.

M が左 R–加群で, R の零元を 0_R, M の零元を 0_M で表すと, (**M1**), (**M2**) より

$$0_R\cdot m = r\cdot 0_M = 0_M \qquad (r\in R,\ m\in M)$$

が成り立つ. また

$$(-r)\cdot m = r\cdot(-m) = -(r\cdot m) \qquad (r\in R,\ m\in M)$$

も成り立つことがわかる.

R が可換で, M が左 R–加群なら

$$m\cdot r = r\cdot m \qquad (r\in R,\ m\in M)$$

とおくと, $m\cdot(r\cdot r') = (m\cdot r)\cdot r'$ が成り立ち, M は右 R–加群ともなる. 同様にして, 右 R–加群より左 R–加群が作れるから, 可換環の場合は左・右の区別をしなくてよい.

例 7.1　A を加法 $+$ に関するアーベル群とする. このとき

$$\boldsymbol{Z}\times A \ni (n, a) \longmapsto n\cdot a = \overbrace{a+\cdots+a}^{n\text{個}} \in A$$

とおくと, これにより A は $\boldsymbol{Z}$–加群となる. したがって, 任意のアーベル群は $\boldsymbol{Z}$–加群とみなせる.

例 7.2　k を $\boldsymbol{R}$ または $\boldsymbol{C}$ とし, V を $\boldsymbol{R}$ または $\boldsymbol{C}$ 上のベクトル空間とする. このとき V は k–加群となる. (実は体 k 上の k–加群のことを k–ベクトル空間 と定義する.)

例 7.3　R を環とし, R を加法により群とみたものを M とおく. このとき R の乗法により, $R\times M \longrightarrow M$, $(r, m)\longmapsto r\cdot m$ が定義される. この演算は, (**M 1**) ～ (**M 4**)

を満たし，M は左 R–加群となる．これにより，環 R は左 R–加群とみなせる．

例 7.4　R を可換環とし，A を R–加群とする．このとき，A に積・：$A \times A \longrightarrow A$ が定義され，この積が分配法則

$$a\cdot(b_1 + b_2) = a\cdot b_1 + a\cdot b_2\,, \qquad (a_1 + a_2)\cdot b = a_1\cdot b + a_2\cdot b$$

$(a, a_1, a_2, b, b_1, b_2 \in A)$ および

$$(r\cdot a)\cdot b = a\cdot(r\cdot b) = r\cdot(a\cdot b) \qquad (r \in R,\ a, b \in A)$$

を満たすとき，A を R 上の **分配多元環** とよぶ．A においては，一般には結合法則は成り立たないが，とくに，結合法則

$$(a\cdot b)\cdot c = a\cdot(b\cdot c) \qquad (a, b, c \in A)$$

が成り立つとき，A を **結合的多元環** とよぶ．さらに結合的多元環 A が乗法に関する単位元をもつとき，A を単に **多元環** という．例えば，$A = M_2(\boldsymbol{R})$ における

$$[X, Y] = X\cdot Y - Y\cdot X \quad や, \qquad X \circ Y = \frac{1}{2}(X\cdot Y + Y\cdot X)$$

は，結合的でない分配多元環としての積を定める．

§8.　代数系と準同型写像

群，環，体，左 R–加群のように，集合の上に有限個の演算が定義され，それらがいくつかの公理(結合法則，分配法則，単位元の存在，逆元の存在など)を満たすものを **代数系** とよぶ．

X_1, X_2 を集合とし，その上にある共通の公理を満たす演算が定義されているものとする．このとき f：$X_1 \longrightarrow X_2$ なる写像は，すべての X_1 の演算を対応する X_2 の演算に対応させるとき，**準同型写像** または **準同型** とよばれる．例えば，G_1, G_2 が共に群のときは，

$$f(a\cdot b) = f(a)\cdot f(b) \qquad (a, b \in G_1)$$

を満たす写像 f：$G_1 \longrightarrow G_2$ が準同型であり，M_1, M_2 が共に左 R–加群のときは，

$$f(m + m') = f(m) + f(m') \qquad (m, m' \in M)$$

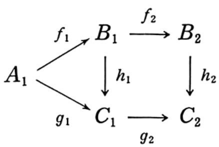
$$f(r\cdot m) = r\cdot f(m) \qquad (r \in R,\ m \in M)$$

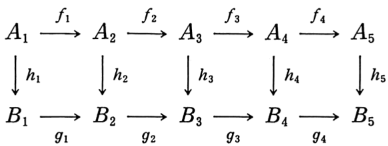
の2条件を満たす写像 $f:\ M_1 \longrightarrow M_2$ が準同型である.

とくに, $f:\ X_1 \longrightarrow X_2$ が全単射な準同型だとする. このとき, 逆写像 $f^{-1}:\ X_2 \longrightarrow X_1$ も全単射な準同型となる. よって, これにより X_1 と X_2 は演算も含めて代数系として同一視できる. 全単射な準同型を **同型** とよび, 代数系 X_1 と X_2 は $f:\ X_1 \longrightarrow X_2$ なる同型写像が存在するとき **同型である** といい $X_1 \simeq X_2$ と表す. 同型という関係は同値関係である.

(注) 準同型のことを準同形, 同型のことを同形 と書くこともある.

代数系の間の写像をいくつか組み合わせて

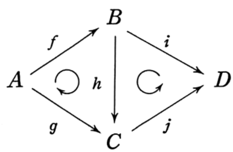




のような **図式** (ダイアグラム) を考えることがある. この場合, これらの図式において, いくつかの準同型を合成したものの間で, 定義域と値域を同じくするものはすべて写像として一致するなら, この図式は **可換** であるという. 例えば右の図式は

$$h \circ f = g, \qquad j \circ h = i$$

のとき可換であり, 右図のような ↻ という記号をつけて表す.



なおこの §8 の概念は, 第VI章でのべる圏と射の概念を使うとより意味が明らかになる.

§9. 多項式環

R を可換環とする. このとき, 文字 x を含む

$$f(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_m x^m + \cdots$$
$$(a_0, a_1, a_2, \cdots, a_m, \cdots \in R,\ m\text{が十分大きいと } a_m = 0)$$

の形の式を，R を係数とする変数（不定元）x の**多項式**という．$m > n$ のとき $a_m = 0$ となるとき，上の様な多項式を

$$f(x) = a_0 + a_1x + \cdots + a_nx^n$$

と書いたり，$f(x) = a_nx^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0$，$f(x) = \sum_{0 \leq m < \infty} a_mx^m$ などと書いたりする．

$$f(x) = \sum_{0 \leq m < \infty} a_m x^m, \qquad g(x) = \sum_{0 \leq m < \infty} b_m x^m$$

を R を係数にもつ変数 x の多項式とする．このとき $f(x)$ と $g(x)$ は，

$$a_0 = b_0, \quad a_1 = b_1, \quad a_2 = b_2, \quad \cdots, \quad a_m = b_m, \quad \cdots$$

が成り立つとき 等しいものと定義する．また $f(x)$ と $g(x)$ の和と積を，

$$f(x) + g(x) = \sum_{0 \leq m < \infty} (a_m + b_m)x^m,$$
$$f(x) \cdot g(x) = \sum_{0 \leq m < \infty} (\sum_{l+n=m} a_l \cdot b_n)x^m$$

で定義する．

R を係数とする変数 x の多項式全体を $R[x]$ で表す．

また R を

$$R \ni a \longmapsto a + 0\,x + 0\,x^2 + \cdots + 0\,x^m + \cdots \in R[x]$$

なる写像により，$R[x]$ の部分集合とみなす．このとき $R[x]$ は，上の和および積に関して，R を含む可換環をなすことがわかる．

$R[x]$ の元 $f(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_m x^m + \cdots$ と $\alpha \in R$ に対し，x を α でおき換えることにより

$$f(\alpha) = a_0 + a_1 \alpha + a_2 \alpha^2 + \cdots + a_m \alpha^m + \cdots$$

という R の元が得られる．$f(\alpha)$ を $f(x)$ に値 α を**代入**した値という．このとき，$\alpha \in R$ を代入することによって得られる写像

$$R[x] \ni f(x) \longmapsto f(\alpha) \in R$$

は，

$$(\sum_{0 \leq m < \infty} a_m \alpha^m) + (\sum_{0 \leq m < \infty} b_m \alpha^m) = \sum_{0 \leq m < \infty} (a_m + b_m)\alpha^m,$$
$$(\sum_{0 \leq m < \infty} a_m \alpha^m) \cdot (\sum_{0 \leq m < \infty} b_m \alpha^m) = \sum_{0 \leq m < \infty} (\sum_{l+n=m} a_l b_n)\, \alpha^m$$

を満たすから，$R[x]$ での和および積を，R での和および積に対応させる．つ

まり，この写像は環の準同型となる．$\alpha \in R$ が $f(\alpha)=0$ を満たすとき，α は多項式 $f(x)$ の **根** であるという．

多項式　$f(x)=a_0+a_1x+\cdots+a_mx^m$　において $a_m \neq 0$ であるとき，m を $f(x)$ の **次数** とよび，$\deg f(x)$ または $\deg f$ と表す．$f(x)=0$ に対しては，$\deg f(x)=-\infty$ とおく．$a_n=0$ かつ $b_n=0$ なら $a_n+b_n=0$ となるから，多項式の和の定義より

$$\deg(f(x)+g(x)) \leqq \max(\deg f(x), \deg g(x))$$

が成り立つ．また

$$f(x)=a_0+a_1x+\cdots+a_mx^m, \qquad g(x)=b_0+b_1x+\cdots+b_nx^n$$

のとき，

$$f(x)\cdot g(x) = (x\text{の}\ (m+n-1)\ \text{次以下の式}) + a_mb_nx^{m+n}$$

となる．よって

$$\deg(f(x)\cdot g(x)) \leqq \deg f(x) + \deg g(x)$$

が成り立つ．

さらに，R が整域であるか，$f(x)$ の最高次の係数 a_m と $g(x)$ の最高次の係数 b_n のどちらか 1 つは零因子でないとする．このとき

$$a_m \neq 0,\ b_n \neq 0 \implies a_m\cdot b_n \neq 0$$

が成り立つから，

$$\deg(f(x)\cdot g(x)) = \deg f(x) + \deg g(x)$$

が成り立つ．とくに，R が整域なら $R[x]$ も整域となる．

多項式環については，除法の一意性を示す次の定理が重要である．

定 理 9. 1　可換環 R を係数とする多項式 $f(x)$，$g(x)$ において，$g(x)$ の最高次の係数が単数であるとする．このとき，$R[x]$ の元 $q(x)$ と $r(x)$ で

$$f(x) = q(x)g(x) + r(x)$$

$$\deg r(x) < \deg g(x)$$

となるものが唯一つ存在する．

一般に，$f(x), g(x) \in R[x]$ が与えられたとき，この2条件を満たす $q(x)$, $r(x) \in R[x]$ が唯一つ存在するなら，$q(x)$ と $r(x)$ をそれぞれ $f(x)$ を $g(x)$ で割った**商**と**余り**という．とくに $f(x) = q(x)g(x)$ となる $q(x) \in R[x]$ が存在するとき，$f(x)$ は $g(x)$ で**割り切れる**という．

[定理の証明] $f(x) = a_0 + a_1 x + \cdots + a_m x^m$ $(a_m \neq 0)$, $g(x) = b_0 + b_1 x + \cdots + b_n x^n$ (b_n は R の単数）とし，$m = \deg f(x)$ に関する帰納法で定理のような $q(x)$ と $r(x)$ を作る．

$m < n$ なら $q(x) = 0$, $r(x) = f(x)$ とおけばよい．$m \geqq n$ であるとし，b_n の逆元を b_n^{-1} とし，

$$h(x) = f(x) - a_m b_n^{-1} x^{m-n} g(x)$$

とおく．このとき，$h(x)$ は m 次の項が消し合って0となるから，$\deg h(x) < \deg f(x)$ となり，帰納法の仮定より

$$h(x) = q_1(x)g(x) + r_1(x), \qquad \deg r_1(x) < \deg g(x)$$

を満たす $q_1(x), r_1(x) \in R[x]$ が存在する．このとき

$$f(x) = (a_m b_n^{-1} x^{m-n} + q_1(x))g(x) + r_1(x)$$

となるから，$q(x) = a_m b_n^{-1} x^{m-n} + q_1(x)$, $r(x) = r_1(x)$ とおくと定理の条件を満たす．

つぎに $q^*(x), r^*(x) \in R[x]$ も

$$f(x) = q^*(x)g(x) + r^*(x), \qquad \deg r^*(x) < \deg g(x)$$

を満たしたとする．この式から $f(x) = q(x)g(x) + r(x)$ を引くと，

$$(q^*(x) - q(x))g(x) = -r^*(x) + r(x)$$

となる．ここで $g(x)$ の最高次の係数は単数だから，$q^*(x) \neq q(x)$ なら

$$\deg\{(q^*(x) - q(x))\cdot g(x)\} \geqq \deg g(x)$$

となる．ところが

$$\deg(-r^*(x) + r(x)) \leqq \max\{\deg r^*(x), \deg r(x)\} < \deg g(x)$$

であるから，これは矛盾である．よって $q^*(x) = q(x)$ となり，$r^*(x) = r(x)$ ともなる． （証明終）

この定理の応用として次の系がでる．

系 9．2 （剰余定理） R を可換環，$f(x)$ を $R[x]$ の元，α を R の元とす

る．このとき $q(x) \in R[x]$ で

$$f(x) = q(x)(x-\alpha) + f(\alpha)$$

を満たすものが唯一つ存在する．

［証 明］ $x-\alpha$ は1次式で，その最高次の係数は1だから R の単数である．よって定理より

$$f(x) = q(x)(x-\alpha) + r(x), \qquad \deg r(x) < 1$$

となる $q(x), r(x) \in R[x]$ が存在する．$\deg r(x) = 0$ または $-\infty$ であるから $r(x)$ は定数である．よって上式に $x=\alpha$ を代入して $f(\alpha) = r(x)$ を得る． （証明終）

この定理より，

$$x-\alpha \text{ が } f(x) \text{ を割り切る} \iff f(\alpha) = 0$$

が成り立つことがわかる．

問 題 9．3 R が整域なら，n 次多項式 $f(x) \in R[x]$ の根の個数は，高々 n 個であることを示せ．

一般に，n を自然数とするとき，n 個の変数 $x_1, x_2, \cdots, x_n$ の R 係数の多項式全体のなす環 $R[x_1, x_2, \cdots, x_n]$ は，帰納的に

$$R[x_1, x_2, \cdots, x_n] = (R[x_1, x_2, \cdots, x_{n-1}])[x_n]$$

として定義される．$R[x_1, x_2, \cdots, x_n]$ の元は

$$f(x_1, x_2, \cdots, x_n) = \sum a_{i_1 i_2 \cdots i_n} x_1{}^{i_1} x_2{}^{i_2} \cdots x_n{}^{i_n}$$

$(a_{i_1 i_2 \cdots i_n} \in R)$ の形で表される．ここで $(i_1, i_2, \cdots, i_n)$ は負でない整数の組全体を動き，有限個以外は $a_{i_1 i_2 \cdots i_n} = 0$ となるものとする．

問 題 9．4 R を無限個の元を含む整域，$f(x_1, x_2, \cdots, x_n), g(x_1, x_2, \cdots, x_n) \in R[x_1, x_2, \cdots, x_n]$ とする．もし多項式として

$$f(x_1, x_2, \cdots, x_n) \neq g(x_1, x_2, \cdots, x_n)$$

なら，R の元の組 $(\alpha_1, \alpha_2, \cdots, \alpha_n)$ で

$$f(\alpha_1, \alpha_2, \cdots, \alpha_n) \neq g(\alpha_1, \alpha_2, \cdots, \alpha_n)$$

となるものが存在することを，n に関する帰納法で示せ．

§10.　行　列

10.1　行列の演算　Rを環，m,nを自然数とする．このとき，Rのmn個の元 a_{ij} $(1 \leqq i \leqq m,\ 1 \leqq j \leqq n)$ を次のように並べたものを，Rに成分をもつ $m \times n$ 型の**行列**という：

$$A = \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \multicolumn{4}{c}{\dotfill} \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{pmatrix}.$$

これを略して　$A = (a_{ij})_{\substack{1\leqq i\leqq m \\ 1\leqq j\leqq n}}$ と書いたり $A = (a_{ij})$　と書いたりする．また a_{ij} を A の (i,j) **成分**といい，A の一部をとり出して作った

$$(a_{i1}, a_{i2}, \cdots, a_{in}) \qquad (1 \leqq i \leqq m)$$

を，行列 A の**第 i 行**とよび，同様にして $a_{1j}, a_{2j}, \cdots, a_{mj}$ $(1 \leqq j \leqq n)$ を縦に並べたものを**第 j 列**とよぶ．

R に成分をもつ $m \times n$ 型の行列の全体を $M(m,n;R)$ で表す．$A = (a_{ij})$，$B = (b_{ij})$ を $M(m,n;R)$ の元とする．このとき，A と B の**和**を，成分ごとの和

$$A + B = \begin{pmatrix} a_{11}+b_{11} & a_{12}+b_{12} & \cdots & a_{1n}+b_{1n} \\ a_{21}+b_{21} & a_{22}+b_{22} & \cdots & a_{2n}+b_{2n} \\ \multicolumn{4}{c}{\dotfill} \\ a_{m1}+b_{m1} & a_{m2}+b_{m2} & \cdots & a_{mn}+b_{mn} \end{pmatrix}$$

として定義する．また $\lambda \in R$ の左からの作用を，

$$\lambda A = \begin{pmatrix} \lambda a_{11} & \lambda a_{12} & \cdots & \lambda a_{1n} \\ \lambda a_{21} & \lambda a_{22} & \cdots & \lambda a_{2n} \\ \multicolumn{4}{c}{\dotfill} \\ \lambda a_{m1} & \lambda a_{m2} & \cdots & \lambda a_{mn} \end{pmatrix}$$

で定義する．これにより $M(m,n;R)$ には左 R–加群の構造が入る．$\lambda\in R$ の右からの作用 $A\lambda$ も同様にして定義される．

l,m,n を自然数とし，$M(l,m;R)$ の元 A と $M(m,n;R)$ の元との行列としての **積** $A\cdot B\in M(l,n;R)$ を次のようにして定義する．

$$c_{ik}=\sum_{1\leqq j\leqq m}a_{ij}\cdot b_{jk}\qquad(1\leqq i\leqq l,\ 1\leqq k\leqq n),$$

$$A\cdot B=\begin{pmatrix}c_{11}&c_{12}&\cdots&c_{1n}\\c_{21}&c_{22}&\cdots&c_{2n}\\\cdots&\cdots&\cdots&\cdots\\c_{l1}&c_{l2}&\cdots&c_{ln}\end{pmatrix}.$$

積 $A\cdot B$ は，A の列の数と B の行の数が等しいときに限り定義される．

とくに，$n\times n$ 型の行列を n 次正方行列とよび，その全体を $M_n(R)$ で表す．A,B を共に $M_n(R)$ の元とすると，A,B の行列としての積 $A\cdot B$ と $B\cdot A$ が定義され，これにより $M_n(R)$ は環となる．ここで $M_n(R)$ の単位元は **単位行列**

$$E_n=\begin{pmatrix}1&0&\cdots&0\\0&1&\cdots&0\\\cdots&\cdots&\cdots&\cdots\\0&0&\cdots&1\end{pmatrix}$$

により与えられる．$M_n(R)$ の元 A は，$M_n(R)$ において逆元をもつとき **正則行列** とよばれ，その逆元を A^{-1} で表し，**逆行列** とよぶ．

問題 10.1 R において結合法則，分配法則が成り立つことを使って，

$$A\in M(k,l;R),\ B\in M(l,m;R),\ C\in M(m,n;R)$$

について結合法則

$$A\cdot(B\cdot C)=(A\cdot B)\cdot C$$

が成り立つことを示せ．

10.2 行列式 R を可換環とする．R に成分をもつ n 次正方行列 $A=$

(a_{ij}) に対して，

$$\det(A) = \sum_{\sigma \in S_n} \mathrm{sgn}(\sigma) \cdot a_{1\sigma(1)} \cdot a_{2\sigma(2)} \cdot \cdots \cdot a_{n\sigma(n)}$$

を行列 A の **行列式** という．ここで S_n は n 次対称群とし，$\mathrm{sgn}(\sigma)$ は $\sigma \in S_n$ の符号とする（例5.6を参照せよ）．

$\det(A)$ を $|A|$ または

$$\begin{vmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \cdots & \cdots & \cdots & \cdots \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{vmatrix}$$

とも表す．

例 10.2 $S_2 = \{(1), (1\ 2)\}$ で $\mathrm{sgn}(1) = 1$, $\mathrm{sgn}(1\ 2) = -1$ だから

$$\begin{vmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{vmatrix} = a_{11}a_{22} - a_{12}a_{21}$$

となる．同様にして，$S_3 = \{(1), (1\ 2\ 3), (1\ 3\ 2), (1\ 2), (2\ 3), (3\ 1)\}$ より具体的に計算すると，次のようになる．

$$\begin{vmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{vmatrix} = a_{11}a_{22}a_{33} + a_{12}a_{23}a_{31} + a_{13}a_{21}a_{32} \\ - a_{13}a_{22}a_{31} - a_{12}a_{21}a_{33} - a_{11}a_{23}a_{32}.$$

例 10.3 $A = (a_{ij}) \in M(m, n; R)$ の行と列を入れ替えたものを ${}^tA = (a_{ji}) \in M(n, m; R)$ と表し，A の **転置行列** という：

$$^t\begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \cdots & \cdots & \cdots & \cdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{pmatrix} = \begin{pmatrix} a_{11} & a_{21} & \cdots & a_{m1} \\ a_{12} & a_{22} & \cdots & a_{m2} \\ \cdots & \cdots & \cdots & \cdots \\ a_{1n} & a_{2n} & \cdots & a_{mn} \end{pmatrix}.$$

このとき

$${}^t({}^tA) = A, \qquad {}^t(A+B) = {}^tA + {}^tB, \qquad {}^t(A \cdot B) = {}^tB \cdot {}^tA$$

などが成り立つ．

A を n 次正方行列とする．$\det A$ の定義において，右辺の積の順序を変えると

$$\det(A) = \sum_{\sigma\in S_n} \mathrm{sgn}(\sigma)\, a_{k_1\sigma(k_1)}\, a_{k_2\sigma(k_2)} \cdots a_{k_n\sigma(k_n)}$$

と書ける．ここで $(k_1, k_2, \cdots, k_n)$ は $(1, 2, \cdots, n)$ の順序を任意に入れ替えたものとする．そこで $k_i = \sigma^{-1}(i)$ となるように k_i をとる．$\tau = \sigma^{-1}$ とおくと，

$$\mathrm{sgn}(\sigma^{-1}) = \mathrm{sgn}(\sigma)$$

が成り立つ．また σ が S_n を動くとき $\tau = \sigma^{-1}$ も S_n を動くから，上式より

$$\det(A) = \sum_{\tau\in S_n} \mathrm{sgn}(\tau)\, a_{\tau(1)\,1} a_{\tau(2)\,2} \cdots a_{\tau(n)\,n} = \det({}^tA)$$

となる．

例 10. 4 $A = (a_{ij}) \in M_n(R)$ の第 i 行と第 j 行が等しいとする．このとき $\sigma\in S_n$ と $\tau = \sigma\cdot(i\ j) \in S_n$ に対し

$$a_{i\,\tau(i)}\cdot a_{j\,\tau(j)} = a_{i\,\sigma(j)}\cdot a_{j\,\sigma(i)} = a_{i\,\sigma(i)}\cdot a_{j\,\sigma(j)}$$

が成り立つ．他方 $\mathrm{sgn}(\tau) = \mathrm{sgn}(\sigma)\,\mathrm{sgn}(i\ j) = -\mathrm{sgn}(\sigma)$ であるから，

$$\mathrm{sgn}(\sigma)\, a_{1\sigma(1)} a_{2\sigma(2)} \cdots a_{n\sigma(n)} + \mathrm{sgn}(\tau)\, a_{1\tau(1)} a_{2\tau(2)} \cdots a_{n\tau(n)} = 0$$

が成り立つ．S_n の元を σ と $\sigma\cdot(i\ j) = \tau$ を組にして考えると，σ から $\det(A)$ へでてくる項と τ からでてくる頂が消し合って

$$\det(A) = 0$$

となる．A の第 i 列と第 j 列が等しいときも，例 10.3 より $\det(A) = 0$ となる．

これより，$A = (a_{ij}) \in M_n(R)$ の第 i 行と第 j 行を共に $(a_{i1} + a_{j1}, a_{i2} + a_{j2}, \cdots, a_{in} + a_{jn})$ でおき換えた行列の行列式

$$\begin{vmatrix} \multicolumn{4}{c}{\cdots\cdots\cdots\cdots} \\ a_{i1} + a_{j1} & a_{i2} + a_{j2} & \cdots & a_{in} + a_{jn} \\ \multicolumn{4}{c}{\cdots\cdots\cdots\cdots} \\ a_{i1} + a_{j1} & a_{i2} + a_{j2} & \cdots & a_{in} + a_{jn} \\ \multicolumn{4}{c}{\cdots\cdots\cdots\cdots} \end{vmatrix}$$

$$= \begin{vmatrix} \multicolumn{4}{c}{\cdots\cdots\cdots} \\ a_{i1} & a_{i2} & \cdots & a_{in} \\ \multicolumn{4}{c}{\cdots\cdots\cdots} \\ a_{i1} & a_{i2} & \cdots & a_{in} \\ \multicolumn{4}{c}{\cdots\cdots\cdots} \end{vmatrix} + \begin{vmatrix} \multicolumn{4}{c}{\cdots\cdots\cdots} \\ a_{i1} & a_{i2} & \cdots & a_{in} \\ \multicolumn{4}{c}{\cdots\cdots\cdots} \\ a_{j1} & a_{j2} & \cdots & a_{jn} \\ \multicolumn{4}{c}{\cdots\cdots\cdots} \end{vmatrix}$$

$$
+\begin{vmatrix} \cdots\cdots\cdots\cdots\cdots \\ a_{j1} & a_{j2} & \cdots & a_{jn} \\ \cdots\cdots\cdots\cdots\cdots \\ a_{i1} & a_{i2} & \cdots & a_{in} \\ \cdots\cdots\cdots\cdots\cdots \end{vmatrix} + \begin{vmatrix} \cdots\cdots\cdots\cdots\cdots \\ a_{j1} & a_{j2} & \cdots & a_{jn} \\ \cdots\cdots\cdots\cdots\cdots \\ a_{j1} & a_{j2} & \cdots & a_{jn} \\ \cdots\cdots\cdots\cdots\cdots \end{vmatrix}
$$

の左辺および右辺の第1項と第4項は0となる．よって行列の2つの行を入れ替えると，行列式の符号は変る．列についても同様である．これより，例5.6の最後の注意を使うと，行列 $A \in M_n(R)$ の行または列に置換 $\tau \in S_n$ を行うと，行列式 $\det(A)$ は $\operatorname{sgn}(\tau)\det(A)$ に変ることがわかる．

例10.4の結果を使うと，次の定理が得られる．

定理 10.5　$A, B \in M_n(R)$ とすると

$$
\det(A \cdot B) = \det(A)\det(B)
$$

が成り立つ．したがって A が正則行列なら $\det(A)$ は R の単数となる．

［証明］　単位行列 E_n の行列式は1であるから，後半は前半より明らかである．

$A=(a_{ij})$，$B=(b_{ij})$ とすると，

$$
A \cdot B = (c_{ij}), \qquad c_{ij} = \sum_{1 \le k_j \le n} a_{i k_j} b_{k_j j}
$$

となる．そこで，行列式が各列について1次同次式となっていることを使い，det と和の順序を入れ替えると，

$$
\det(A \cdot B) = \sum_{1 \le k_1, k_2, \cdots, k_n \le n} \begin{vmatrix} a_{1k_1} & a_{1k_2} & \cdots & a_{1k_n} \\ a_{2k_1} & a_{2k_2} & \cdots & a_{2k_n} \\ \cdots\cdots\cdots\cdots\cdots \\ a_{nk_1} & a_{nk_2} & \cdots & a_{nk_n} \end{vmatrix} b_{k_1 1} b_{k_2 2} \cdots b_{k_n n}
$$

となる．ここで $k_1, k_2, \cdots, k_n$ のうち等しいものがあれば，右辺の行列式が0となる．よって和は $\{k_1, k_2, \cdots, k_n\} = \{1, 2, \cdots, n\}$ を満たす組を動くものとしてよい．そこで

$$
\sigma = \begin{pmatrix} 1 & 2 & \cdots & n \\ k_1 & k_2 & \cdots & k_n \end{pmatrix}
$$

とおくと，例10.4の最後の注意より，

$$\det(A\cdot B)=\sum_{\sigma\in S_n}\operatorname{sgn}(\sigma)\begin{vmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \cdots & \cdots & \cdots & \cdots \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{vmatrix} b_{\sigma(1)1}b_{\sigma(2)2}\cdots b_{\sigma(n)n}$$

が成り立つ．これは例 10.3 より $\det(A)\cdot\det(B)$ に等しい． (証明終)

$A=(a_{ij})$ を $M_n(R)$ の元とし，A より第 i 行と第 j 列をとり去って得られる $(n-1)$ 次正方行列の行列式に $(-1)^{i+j}$ を掛けたものを a_{ij} の **余因子** とよび，$\varDelta_{ij}$ と表す：

$$\varDelta_{ij}=(-1)^{i+j}\begin{vmatrix} a_{11} & \cdots & a_{1\,j-1} & a_{1\,j+1} & \cdots & a_{1n} \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ a_{i-1\,1} & \cdots & a_{i-1\,j-1} & a_{i-1\,j+1} & \cdots & a_{i-1\,n} \\ a_{i+1\,1} & \cdots & a_{i+1\,j-1} & a_{i+1\,j+1} & \cdots & a_{i+1\,n} \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ a_{n1} & \cdots & a_{n\,j-1} & a_{n\,j+1} & \cdots & a_{nn} \end{vmatrix}.$$

このとき次の定理が成り立つ．

定理 10. 6 $1\leqq s,t\leqq n$ とし，$A=(a_{ij})\in M_n(R)$ なる行列での a_{ij} の余因子を $\varDelta_{ij}$ で表す．このとき

$$\det(A)=\sum_{1\leqq l\leqq n}a_{sl}\varDelta_{sl}=\sum_{1\leqq l\leqq n}a_{lt}\varDelta_{lt}$$

が成り立つ．

[証明] $\varDelta_{ij}$ を A の関数とみて $\varDelta_{ij}(A)$ と表す．x_{ij} $(1\leqq i,j\leqq n)$ を R 上の変数として R 上の多項式環 $R[x_{ij}\mid 1\leqq i,j\leqq n]$ に成分をもつ行列 $X=(x_{ij})$ に対して定理を証明する．そうすると，R は可換環だから，$X=(x_{ij})$ に任意の R に成分をもつ行列 $A=(a_{ij})$ を代入しても定理は成り立つ．

$$\det(X)=\sum_{\sigma\in S_n}\operatorname{sgn}(\sigma)\,x_{1\sigma(1)}x_{2\sigma(2)}\cdots x_{n\sigma(n)}$$

を $x_{s1},x_{s2},\cdots,x_{sn}$ について整理すると，

$$\det(X)=y_1x_{s1}+y_2x_{s2}+\cdots+y_nx_{sn}$$

$(y_1,y_2,\cdots,y_n\in R[x_{ij}\mid 1\leqq i,\ j\leqq n,\ i\neq s])$ と書ける．ここで $x_{sk}=1,\ x_{sl}=0$ $(l\neq k)$ とおくと

$$y_k = \begin{vmatrix} x_{11} & \cdots & x_{1k} & \cdots & x_{1n} \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ 0 & \cdots & 1 & \cdots & 0 \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ x_{n1} & \cdots & x_{nk} & \cdots & x_{nn} \end{vmatrix}$$

と行列 X の第 i 行を $(0, \cdots, 1, \cdots, 0)$ でおき替えた行列の行列式がでてくる．そこでこの行列の行に巡回置換 $\sigma = (s, s+1, \cdots, n)$ を行い，列に巡回置換 $\tau = (k, k+1, \cdots, n)$ を行う．このとき $\mathrm{sgn}(\sigma) = (-1)^{n-s}$, $\mathrm{sgn}(\tau) = (-1)^{n-k}$ であるから，例 10.4 より

$$y_k = (-1)^{s+k} \begin{vmatrix} a_{11} & \cdots & a_{1n} & a_{1k} \\ \cdots & \cdots & \cdots & \cdots \\ a_{n1} & \cdots & a_{nn} & a_{nk} \\ 0 & \cdots & 0 & 1 \end{vmatrix}$$

となる．この右辺を行列式の定義に従って展開すると，$\sigma(n) = n$ となる $\sigma \in S_n$ についての和のみが残り，他は 0 となる．そこで，このような S_n の元全体と S_{n-1} の元全体を同一視すると，

$$y_k = (-1)^{s+k} \begin{vmatrix} a_{11} & \cdots & a_{1n} \\ \cdots & \cdots & \cdots \\ a_{n1} & \cdots & a_{nn} \end{vmatrix} \qquad (s \text{ 行と } k \text{ 列は除かれている})$$

となる．よって y_k は $X = (x_{ij})$ における x_{ik} の余因子となり，

$$\det(X) = \sum_{1 \leq l \leq n} x_{sl} \Delta_{sl}(X) \qquad \cdots\cdots\cdots\cdots\cdots(*)$$

が成り立つ．

$$\det(X) = \sum_{1 \leq l \leq n} x_{lt} \Delta_{lt}(X) \qquad \cdots\cdots\cdots\cdots\cdots(**)$$

も同様にして得られる．（証明終）

この定理の証明にでてきた式 $(*)$ において，$1 \leqq t \leqq n$, $t \neq s$ として $x_{ij} = a_{ij}\ (1 \leqq i, j \leqq n,\ i \neq t)$, $x_{tj} = a_{sj}\ (1 \leqq j \leqq n)$ とおくと，$A = (a_{ij})$ において，第 t 行を第 s 行でおき換えた行列の行列式が $a_{s1}\Delta_{t1} + a_{s2}\Delta_{t2} + \cdots + a_{sn}\Delta_{tn}$ に等しいことがわかる．ところが例 10.4 よりこの行列式は 0 に等しいから

$$a_{s1}\Delta_{t1} + a_{s2}\Delta_{t2} + \cdots + a_{sn}\Delta_{tn} = 0 \qquad (1 \leqq s, t \leqq n,\ s \neq t)$$

が成り立つ．同様に $(**)$ より

$$a_{1s}\Delta_{1t} + a_{2s}\Delta_{2t} + \cdots + a_{ns}\Delta_{nt} = 0 \qquad (1 \leqq s, t \leqq n,\ s \neq t)$$

が得られる．定理とこの 2 式をまとめると次のようになる．

系 10.7 Rを可換環，$A=(a_{ij})\in M_n(R)$，Aにおけるa_{ij}の余因子をΔ_{ij}，$\Delta=(\Delta_{ji})\in M_n(R)$ とする．このとき，単位行列をE_nとすると

$$A\cdot\Delta=\Delta\cdot A=\det(A)\cdot E_n$$

が成り立つ．

この系において，$\det(A)$ が単数なら $A^{-1}=\det(A)^{-1}\Delta$ とおくと $AA^{-1}=A^{-1}A=E_n$ となる．よって

系 10.8 Rを可換環，$A\in M_n(R)$ とする．このときAが正則行列となるための必要十分条件は，$\det(A)$ がRの単数となることである．

例 10.9 Rを可換環とし，Rに成分をもつn次正則行列の全体を $GL_n(R)$ で表す．系 10.8 より

$$GL_n(R)=\{A\in M_n(R)\mid \det(A)\ \text{は}\ R\ \text{の単数}\}$$

となる．したがって $GL_n(R)$ は

$$SL_n(R)=\{A\in M_n(R)\mid \det(A)=1\}$$

を部分集合として含む．$GL_n(R)$ と $SL_n(R)$ は，行列の積により，単位行列E_nを単位元とする群をなす．これらをそれぞれ，R上の **n 次一般線型群**，R上の **n 次特殊線型群** とよぶ．

例 10.10 Rを可換環とし，$A=(a_{ij})\in M_n(R)$ とする．このとき，xについての多項式

$$f_A(x)=\det(xE_n-A)\in R[x]$$

を，Aの **固有多項式** または **特性多項式** とよぶ．定義より明らかに，固有多項式 $f_A(x)$ は，Aを PAP^{-1} $(P\in GL_n(R))$ でおき換えても変らない．

$f_A(x)$ をxの多項式とみて展開すると，

$$f_A(x)=x^n-\mathrm{tr}(A)\,x^{n-1}+\cdots+(-1)^n\det(A)$$

の形となる．ここで

$$\mathrm{tr}(A)=\sum_{1\leq i\leq n}a_{ij}$$

をAの **トレース** とよぶ．トレースは，

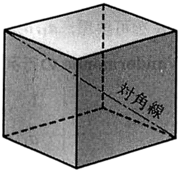
$$\mathrm{tr}(A+B)=\mathrm{tr}(A)+\mathrm{tr}(B),$$
$$\mathrm{tr}(AB)=\mathrm{tr}(BA),$$

$$\mathrm{tr}(PAP^{-1}) = \mathrm{tr}(A)$$

$(A, B \in M_n(R),\ P \in GL_n(R))$ などを満たす．

問　　　題

1.　正六面体においては，向かい合う頂点を結ぶ対角線は4本存在する．これら対角線の置換の群とみることにより，正六面体群は対称群 S_4 と同型になることを示せ．



2.　kを体とし，$n+1$ 個の k の元 $\alpha_1, \alpha_2, \cdots, \alpha_{n+1}$ をとる．このとき，n 次の多項式 $f(x) \in k[x]$ で，与えられた点 α_i $(i = 1, 2, \cdots, n+1)$ において与えられた値 β_i $(i = 1, 2, \cdots, n+1)$ をとるものを作れ．

3.　Rを可換環とし，xを変数とする．$a_1, a_2, \cdots, a_n \in R$ に対し

$$(x-a_1)(x-a_2)\cdots(x-a_n) = x^n - s_1 x^{n-1} + s_2 x^{n-2} - \cdots + (-1)^n s_n$$

で $a_1, a_2, \cdots, a_n$ の **基本対称式**

$$s_1 = a_1 + a_2 + \cdots + a_n$$
$$s_2 = a_1 a_2 + a_1 a_3 + \cdots + a_2 a_3 + \cdots + a_{n-1} a_n$$
$$\cdots\cdots\cdots\cdots\cdots\cdots$$
$$s_n = a_1 a_2 \cdots a_n$$

を定義する．また m を自然数とするとき

$$\sigma_m = a_1{}^m + a_2{}^m + \cdots + a_n{}^m$$

とおく．このとき

（1）
$$\sigma_m - \sigma_{m-1} s_1 + \sigma_{m-2} s_2 - \cdots + (-1)^{m-1} \sigma_1 s_{m-1} + (-1)^m m s_m = 0 \qquad (m \leqq n)$$
$$\sigma_m - \sigma_{m-1} s_1 + \sigma_{m-2} s_2 - \cdots + (-1)^n \sigma_{m-n} s_n = 0 \qquad (m > n)$$

が成り立つことを示せ．

（2）　$R = \boldsymbol{C}$ とする．$\sigma_m \in \boldsymbol{Q}$ $(m = 1, 2, \cdots)$ なら $s_1, s_2, \cdots, s_n \in \boldsymbol{Q}$ となることを示せ．（$\sigma_m \in \boldsymbol{Z}$ なら，$s_i \in \boldsymbol{Z}$ となる．）

4． 可換環 R 上の行列 $A \in M_n(R)$ を $A = \begin{pmatrix} A_1 & A_2 \\ A_3 & A_4 \end{pmatrix}$ と $A_1 \in M_{n_1}(R)$，$A_2 \in M(n_1, n_2; R)$，$A_3 \in M(n_2, n_1; R)$，$A_4 \in M_{n_2}(R)$ のブロックに分けたとき，A_3 が零行列となったとする．このとき

$$\det(A) = \det(A_1)\cdot\det(A_4)$$

が成り立つことを示せ．

5． R を可換環，$a_1, a_2, \cdots, a_n \in R$ とする．このとき，次の等式が成り立つことを示せ．(**Vandermonde の行列式** とよばれる．)

$$\begin{vmatrix} 1 & 1 & \cdots & 1 \\ a_1 & a_2 & \cdots & a_n \\ \cdots & \cdots & \cdots & \cdots \\ a_1^{n-1} & a_2^{n-1} & \cdots & a_n^{n-1} \end{vmatrix} = (-1)^{\frac{n(n-1)}{2}} \prod_{i<j} (a_i - a_j).$$

6． $a_1, a_2, \cdots, a_n \in \boldsymbol{C}$ とするとき

$$\begin{vmatrix} a_1 & a_2 & \cdots & a_{n-1} & a_n \\ a_n & a_1 & \cdots & a_{n-2} & a_{n-1} \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ a_3 & a_4 & \cdots & a_1 & a_2 \\ a_2 & a_3 & \cdots & a_n & a_1 \end{vmatrix} = \prod_{\zeta^n=1} (a_1 + \zeta a_2 + \cdots + \zeta^{n-2} a_{n-1} + \zeta^{n-1} a_n)$$

が成り立つことを示せ．

II 群

G が群であるとは，G は集合であり，その上に積とよばれる演算 $G\times G \longrightarrow G$ が定義されており，さらにこの演算が結合法則，単位元の存在，逆元の存在という3つの公理を満たすことをいった（第I章，§5参照）．この章では群の性質を詳しく調べる．なお群の表現についての話は，半単純環の理論の応用として，第IV章でのべる．

§1. 部分群と剰余類

1.1 部分群　G を群とし，H を G の空でない部分集合とする．このとき H が G の**部分群**であるとは，H が G の演算により群となることをいう．結合法則は G で成り立てば H でも成り立つから，これは

(SG 1)　　$a, b\in H \implies a\cdot b\in H$,

(SG 2)　　$a\in H \implies a^{-1}\in H$

の2つが成り立つことを意味する．逆に $G\supset H\neq \emptyset$ について (SG 1), (SG 2) が成り立つとする．このとき積は $H\times H\longrightarrow H$ なる写像をひきおこす．さらに $a\in H$ より，$a^{-1}\in H$ と $1=a\cdot a^{-1}\in H$ が導かれるから，H は G での積により群となる．よって (SG 1), (SG 2) は H が G の部分群となるための必要十分条件を与える．

A, B を群 G の部分集合とする．このとき

$$A\cdot B=\{a\cdot b \mid a\in A, b\in B\},$$
$$A^{-1}=\{a^{-1} \mid a\in A\}$$

で G の部分集合 $A \cdot B$ と A^{-1} を定義する．この記号を使うと，H が G の部分群となるための条件は

$$H \cdot H \subset H, \qquad H^{-1} \subset H$$

と書ける．$H \ni 1$ および $(H^{-1})^{-1} = H$ を使うと，ここでの $\subset$ は，実は等号であることがわかる．

G を群とすると，G および，単位元のみから成る群 $\{1\}$ は常に G の部分群となる．これらを **自明な部分群** とよび，G 以外の部分群を **真部分群** とよぶ．

例 1．1　G を群とする．このとき

$$Z(G) = \{a \in G \mid ax = xa \ (\forall x \in G)\}$$

とおくと，$Z(G)$ は G の部分群となる．これを G の **中心** とよぶ．

例 1．2　G を整数の加法のなす群 $\boldsymbol{Z}$ とし，H を G の自明でない部分群とする．m を H に入る最小の正整数とし，n を H の任意の元とする．n を m で割り $n = qm + r$, $0 \leqq r < m$ $(q, r \in \boldsymbol{Z})$ と書く．このとき $r = n - qm \in H$ となるから，m の最小性より $r = 0$ となる．よって m を上のようにとると，$H = m\boldsymbol{Z} = \{ma \mid a \in \boldsymbol{Z}\}$ となる．

例 1．3　R を可換環とし，$GL_n(R)$ を R に成分をもつ n 次正則行列全体のなす群，$SL_n(R) = \{A \in M_n(R) \mid \det(A) = 1\}$ とおく．このとき $SL_n(R)$ は $GL_n(R)$ の部分群となる（第Ⅰ章，例 10.9 参照）．また

$$O_n(R) = \{A \in M_n(R) \mid {}^tA \cdot A = A \cdot {}^tA = E_n\}$$

とおくと，これも $GL_n(R)$ の部分群となる．これを n 次 **直交群** とよぶ．つぎに

$$S_p(n\,; R) = \{B \in M_{2n}(R) \mid {}^tB \cdot J \cdot B = J\} \qquad \left(J = \begin{pmatrix} 0 & E_n \\ -E_n & 0 \end{pmatrix} \in M_{2n}(R)\right)$$

とおくと，これも $GL_{2n}(R)$ の部分群となる．これを n 次 **シンプレクティック群** とよぶ．これらの群は，Lie 群論や代数群論において非常に重要な群である．

問題 1．4　H, K を G の部分群とするとき，次を示せ．

（1）　$H \cap K$ も G の部分群である．

（2）　$H \cdot K$ が G の部分群 $\iff$ $H \cdot K = K \cdot H$.

S を群 G の部分集合とする．このとき S の元の有限個のべき積 $a_1^{m_1} a_2^{m_2} \cdots$

${a_n}^{m_n}$ $(n, m_i \in \boldsymbol{Z},\ a_i \in S)$ の全体は，S を含む G の 部分群となる．これを $\langle S \rangle$ で表し，S で **生成される部分群** とよぶ．

G の部分群 H は

$$H = \langle a \rangle = \{a^n \mid n \in \boldsymbol{Z}\}$$

と1つの元で生成されるとき **巡回群** であるといい，a を H の **生成元** という．また，G の部分群 H は，有限個の G の元により生成されるとき **有限生成** であるという．

G の部分群 H に対し，H の 元の 個数 $|H|$ を H の **位数** とよぶ．また，$|H| < \infty$ のとき H を **有限部分群**，$|H| = \infty$ のとき **無限部分群** という．とくに $|G| < \infty$ のとき G を **有限群**，$|G| = \infty$ のとき **無限群** という．

a を G の元とする．このとき a で生成された G の部分群 $\langle a \rangle$ の位数を，**元 a の位数** とよび，$o(a)$ で表す．m, n を $m > n$ なる整数とすると，

$$a^m = a^n \iff a^{m-n} = 1$$

が成り立つ．よって $o(a) < \infty$ のときは，$o(a)$ は

$$a^l \neq 1 \ (1 \leqq l < o(a)), \qquad a^{o(a)} = 1$$

となる自然数として定まり，$o(a) = \infty$ のときは，

$$\cdots, \quad a^{-2}, \quad a^{-1}, \quad 1, \quad a, \quad a^2, \quad \cdots$$

はすべて相異なる．

1.2　剰余類　　群 G の 部分群 H に対し，Ha $(a \in G)$ の形の G の部分集合を，G における H の **右剰余類** とよぶ．同様に aH $(a \in G)$ の形の集合を，H の **左剰余類** とよぶ．

（注）Ha を左剰余類，aH を右剰余類とよぶ流儀もあるが，Ha を右剰余類とよぶ方が一般的であるようである．

G の2元 a, b に対し

$$a \sim b \iff Ha = Hb$$

とおくと，この関係 $\sim$ は同値関係となる．この同値関係により G を類別する

と，

$$G = \coprod_{i \in I} Ha_i$$

の形の類別が得られる．これを G の部分群 H による右剰余類への分解といい，G における H の右剰余類の全体を $H \backslash G$ で表す．同様にして，G の H による左剰余類への分解 $G = \coprod_{j \in J} a_j H$，および左剰余類全体の集合 G/H も得られる．

$G \ni x \longmapsto x^{-1} \in G$ は全単射であるから，

$$Ha = Hb \iff a^{-1}H = b^{-1}H$$

が成り立つ．よって

$$G = \coprod_{i \in I} Ha_i \iff G = \coprod_{i \in I} a_i{}^{-1}H$$

が成り立ち，したがって $H \backslash G$ も G/H も同じ個数の元から成る．この共通の個数を $[G : H]$ で表し，G における H の **指数** とよぶ．

定理 1.5（ラグランジェ）　G を有限群，H を G の部分群とする．このとき，

（i）　$|G| = [G : H]|H|$　が成り立つ．

（ii）　部分群 H の位数も指数も，G の位数の約数となる．

［証明］　$G = \coprod_{i \in I} Ha_i$ を G の H による右剰余類への分解とする．このとき $[G : H] = |I|$ となる．

$$H \ni h \longmapsto ha_i \in Ha_i$$

は H より Ha_i への全単射であるから，各剰余類 Ha_i はちょうど $|H|$ 個の元を含む．よって G の元の個数 $|G|$ は $[G : H] \times |H|$ に等しい．(ii) は (i) より明らかである．（証明終）

とくに $H = \langle a \rangle$ ととると，

系 1.6　有限群 G の元の位数は，$|G|$ の約数となる．

例 1.7　G を位数が素数 p の群とする．a を G の 1 以外の元とすると，$\langle a \rangle$ は G の $\{1\}$ 以外の部分群となる．$|G| = p$ だから，ラグランジェの定理より，その約数である $|\langle a \rangle| = o(a)$ は p と一致する．したがって $G = \langle a \rangle$ となり，G は巡回群となる．G は

真の部分群をもたないこともわかった.

例 1.8　m を自然数とし, G を環 $\boldsymbol{Z}/m\boldsymbol{Z}$ の単数群 $U(\boldsymbol{Z}/m\boldsymbol{Z})$ とする. G の元は, $\boldsymbol{Z}/m\boldsymbol{Z}$ の元 $a \pmod m$ のうち, a が m と素なもの全体から成る. $G=U(\boldsymbol{Z}/m\boldsymbol{Z})$ の位数を $\varphi(m)$ で表し, φ を **オイラー関数** とよぶ. このとき, ラグランジェの定理より,

$$a^{\varphi(m)} \equiv 1 \pmod m$$

が成り立つ. とくに, m が素数 p のときは $\varphi(p)=p-1$ であるから, 任意の p で割れない整数 a に対し

$$a^{p-1} \equiv 1 \pmod p$$

が成り立つ. これを **フェルマの小定理** とよぶ.

問題 1.9　G を群, H, K を G の部分群とする. このとき

$$a \sim b \iff HaK = HbK$$

とおくと, これは G における同値関係を与えることを示せ. この同値関係による

$$G = \coprod_{i \in I} Ha_iK$$

なる類別を, G の部分群 H と K による **両側分解** とよぶ.

§2.　正規部分群と準同型定理

2.1　正規部分群　G を群, N を G の部分群とする. このとき

$$aN = Na \qquad (\forall a \in G)$$

が成り立つなら, N は G の **正規部分群** であるといい, $N \lhd G$ と表す. この条件は, $aNa^{-1}=N$ とも書けるから, N が正規部分群であるとは, N が

$$I_a:\ G \ni x \longmapsto axa^{-1} \in G \qquad (a \in G)$$

なる写像で不変なことともいい直せる.

G を群とすると, G 自身および単位群 $\{1\}$ は G の正規部分群となる. これらの他に正規部分群をもたない群を **単純群** とよぶ. 例えば位数が素数の群は単純群である (例 1.7 参照).

N を G の正規部分群とする. このとき $aN=Na$ が成り立つから, $G/N=N\backslash G$ となる. aN, bN を G/N の 2 元とすると, G の部分集合として

$$(aN)(bN) = a(Nb)N = a(bN)N = (ab)(NN) = abN$$

が成り立つ．とくに類 abN は，類 aN と類 bN のみにより，a, b の選び方によらずに定まることがわかる．そこで $(aN, bN) \longmapsto abN$ により

$$G/N \times G/N \longrightarrow G/N$$

なる写像を定め，G/N に積

$$(aN)\cdot(bN) = abN$$

を定義する．

G において結合法則が成り立つから，

$$\begin{aligned}(aN\cdot bN)\cdot cN &= abN\cdot cN = (ab)cN \\ &= a(bc)N = aN\cdot bcN = aN\cdot(bN\cdot cN)\end{aligned}$$

となり，G/N での積に対しても結合法則が成り立つ．また G/N では $1\cdot N = N$ が単位元となり，$a^{-1}N$ が aN の逆元となる．よって G/N は群となる．これを群 G の正規部分群 N による **剰余群** とよぶ．

問題 2.1 G を群とする．

（1） N_1, N_2 が G の正規部分群なら，$N_1 \cap N_2$ も $N_1\cdot N_2$ も G の正規部分群となることを示せ．

（2） H を G の部分群，N を G の正規部分群とするとき，$H \cap N$ は H の正規部分群で，$H\cdot N$ は G の部分群となることを示せ．

2.2 準同型 G, G' を群とする．このとき写像 $f:\ G \longrightarrow G'$ が条件

$$f(a\cdot b) = f(a)\cdot f(b)$$

を満たすなら，f は（群の）**準同型写像**（または **準同型**）であるという（第 I 章，§8 参照）．

$f:\ G \longrightarrow G'$ を準同型写像とし，$1_G, 1_{G'}$ を G, G' の単位元とする．このとき $f(a) = f(a\cdot 1_G) = f(a)\cdot f(1_G)$ が成り立つ．よって両辺に $f(a)^{-1}$ を掛けることにより，

$$f(1_G) = 1_{G'}$$

が成り立つことがわかる．また $f(a)\cdot f(a^{-1}) = f(a\cdot a^{-1}) = f(1_G) = 1_{G'}$ であるから

$$f(a^{-1}) = f(a)^{-1}$$

が成り立つこともわかる．

$$\mathrm{Im}(f) = \{f(a) \mid a \in G\},$$

$$\mathrm{Ker}(f) = \{a \in G \mid f(a) = 1_{G'}\}$$

とおき，各々準同型写像 $f\colon G \longrightarrow G'$ の**像**および**核**とよぶ．準同型写像の定義と，上で見たことより，$\mathrm{Im}(f)$ は G' の部分群となる．また $a, b \in \mathrm{Ker}(f)$ とすると

$$f(a\cdot b) = f(a)\cdot f(b) = 1_{G'}\cdot 1_{G'} = 1_{G'}$$

$$f(a^{-1}) = f(a)^{-1} = (1_{G'})^{-1} = 1_{G'}$$

が成り立つから，$a\cdot b,\ a^{-1} \in \mathrm{Ker}(f)$ となり，$\mathrm{Ker}(f)$ は G の部分群となる．さらに x を G の任意の元とするとき，

$$f(xax^{-1}) = f(x)\cdot f(a)\cdot f(x)^{-1} = f(x)\cdot 1_{G'}\cdot f(x)^{-1} = 1_{G'}$$

となり，$xax^{-1} \in \mathrm{Ker}(f)$ となる．よって $\mathrm{Ker}(f)$ は G の正規部分群となる．

例 2. 2　N を群 G の正規部分群とする．このとき

$$\pi\colon\ G \ni a \longmapsto aN \in G/N$$

は，G より剰余群 G/N への準同型写像となる．これを**自然な準同型**とよぶ．このとき，$\mathrm{Im}(\pi) = G/N$, $\mathrm{Ker}(\pi) = N$ となることは明らかである．これより，N が G の正規部分群となることと，N がある準同型 $f\colon G \longrightarrow G'$ の核となることとが同値なことがわかる．

$f\colon G \longrightarrow G'$ を群の準同型とする．このとき，f が全射であることは，$\mathrm{Im}(f) = G'$ と同値である．また

$$f(a) = f(b) \iff f(a^{-1}b) = 1 \iff a^{-1}b \in \mathrm{Ker}(f)$$

であるから，f が単射となるための必要十分条件は $\mathrm{Ker}(f) = \{1\}$ となることである．全射かつ単射な準同型写像を**同型写像**（または**同型**）とよび，同

型写像 $f\colon\ G \longrightarrow G'$ が存在する群 G と G' を**同型**であるといい，$G \simeq G'$ と表す（第Ⅰ章，§8参照）.

$f\colon\ G \longrightarrow G'$ を群の同型写像とする．このとき逆写像 $f^{-1}\colon\ G' \longrightarrow G$ が定義され，これも同型写像となる．これより，$G \simeq G'$ という関係は同値関係であることがわかる．同型な群は，同じ個数の元を含み，しかも同じ積構造をもつ．この意味で，同型な群を以下同一視する.

次の定理は，群論における準同型写像の意義を示しており，非常に重要である.

定理 2.3（準同型定理） G, G' を群とし，$f\colon\ G \longrightarrow G'$ を準同型写像とする．このとき，$a\,\mathrm{Ker}(f) \longmapsto f(a)$ なる対応により，同型

$$G/\mathrm{Ker}(f) \simeq \mathrm{Im}(f)$$

が得られる．とくに f が全射なら

$$G/\mathrm{Ker}(f) \simeq G'$$

となる．また G の $\mathrm{Ker}(f)$ を含む部分群 H と $\mathrm{Im}(f)$ の部分群 H' とは，

$$H = f^{-1}(H') \longleftrightarrow H' = f(H)$$

なる対応で1対1に対応する.

[証明] 中間部分は前半より明らかである.

$N = \mathrm{Ker}(f)$ とおく．$N \lhd G$ だから G/N は群となる.

$$f(a) = f(b) \iff aN = bN$$

であるから，$\bar{f}(aN) = f(a)$ とおくと，これは a のとり方によらず aN のみで定まり，$\bar{f}\colon\ G/N \longrightarrow \mathrm{Im}(f)$ なる写像が定義される．この写像は明らかに全単射であり，

$$\bar{f}(aN\cdot bN) = \bar{f}(abN) = f(ab) = f(a)f(b) = \bar{f}(aN)\bar{f}(bN)$$

が成り立つから準同型である．よって $\bar{f}\colon\ G/N \longrightarrow \mathrm{Im}(f)$ は同型となる.

H を $\mathrm{Ker}(f)$ を含む G の部分群とする．このとき

$$a \in f^{-1}(f(H)) \iff f(a) \in f(H) \iff a \in H$$

であるから，$f^{-1}(f(H)) = H$ となる．逆に H' を $\mathrm{Im}(f)$ の部分群とすると，$f^{-1}(H') \supset \mathrm{Ker}(f)$，$f(f^{-1}(H')) = H'$ が成り立つ．よって $H \longleftrightarrow H'$ は1対1対応となる.

（証明終）

準同型定理の系として，以下のいくつかの結果が得られる．

系 2. 4　（同型定理）（i）H を G の部分群，N を G の正規部分群とする．このとき

$$NH/N \simeq H/H \cap N.$$

（ii）$f\colon\ G \longrightarrow G'$ を全射な準同型，$H' \lhd G'$，$H = f^{-1}(H')$ とする．このとき

$$G/H \simeq G'/H'.$$

[証 明]（i）問題 2.1 より NH は G の部分群である．$\pi\colon\ G \longrightarrow G/N$ を自然な準同型とし，これを H に制限したものを π_H とする．このとき $\mathrm{Im}(\pi_H) = NH/N$, $\mathrm{Ker}(\pi_H) = H \cap \mathrm{Ker}(\pi) = H \cap N$ が成り立つ．よって準同型定理より，$H/H \cap N \simeq NH/N$ となる．

（ii）f と自然な準同型との合成を $g\colon\ G \longrightarrow G'/H'$ とする．このとき $\mathrm{Im}(g) = G'/H'$，$\mathrm{Ker}(g) = f^{-1}(H') = H$ が成り立つ．よって準同型定理より，$G/H \simeq G'/H'$ となる．（証明終）

系 2. 5　H, N を群 G の正規部分群で $N \subset H$ であるとする．このとき

$$G/H \simeq (G/N)/(H/N).$$

[証 明]　$f\colon\ G/N \ni aN \longmapsto aH \in G/H$ なる全射準同型の核は H/N であるから，準同型定理より求める同型が得られる．（証明終）

例 2. 6　G を a で生成される巡回群とする．このとき

$$f\colon\quad \boldsymbol{Z} \ni n \quad\longmapsto\quad a^n \in G$$

は全射な準同型である．$\mathrm{Ker}(f)$ は $\boldsymbol{Z}$ の部分群だから，例 1.2 より $\mathrm{Ker}(f) = \{0\}$ または $m\boldsymbol{Z}$（m は自然数）となる．よって，準同型定理より，$G \simeq \boldsymbol{Z}$ または $G \simeq \boldsymbol{Z}/m\boldsymbol{Z}$ となる．

H を $\boldsymbol{Z}/m\boldsymbol{Z}$ の部分群とする．自然な準同型 $\pi\colon\ \boldsymbol{Z} \to \boldsymbol{Z}/m\boldsymbol{Z}$ に準同型定理を使うと，$H' \supseteqq m\boldsymbol{Z}$ なる $\boldsymbol{Z}$ の部分群 H' があり $H = \pi(H')$ となることがわかる．H' は $n\boldsymbol{Z}$（n は m の約数）の形だから，$H = n\boldsymbol{Z}/m\boldsymbol{Z}$ となる．これより $\boldsymbol{Z}/m\boldsymbol{Z}$ の指数 m/n の部分群は $n\boldsymbol{Z}/m\boldsymbol{Z}$ に限ることがわかる．なお $\boldsymbol{Z}$ の指数 n の部分群は $n\boldsymbol{Z}$ に限るから，巡回群の部分群は，指数を決めると一意的に定まることもわかった．

例 2. 7 R を可換環とし，$G = GL_n(R)$ を n 次一般線型群とする（第Ⅰ章，例 10.9 参照）．このとき

$$G \ni A \longmapsto \det(A) \in U(R)$$

なる群の準同型を考える．G は $\begin{pmatrix} u & & & 0 \\ & 1 & & \\ & & \ddots & \\ 0 & & & 1 \end{pmatrix}$ $(u \in U(R))$ の形の元を含むから，この写像の像は $U(R)$ と一致する．またこの写像の核は，n 次特殊線型群 $SL_n(R)$ である．よって準同型定理より，$SL_n(R) \lhd GL_n(R)$ かつ $GL_n(R)/SL_n(R) \simeq U(R)$ となる．

2. 3 Hom(G, G') と完全列

G, G' を群とする．このとき，

$$\mathrm{Hom}(G, G') = \{f : G \longrightarrow G' \mid \text{準同型写像}\}$$

とおく．G' がアーベル群なら，$\mathrm{Hom}(G, G')$ は積

$$(f \cdot g)(x) = f(x) \cdot g(x) \qquad (f, g \in \mathrm{Hom}(G, G'),\ x \in G)$$

により乗法群をなす．また写像の合成 $(f, g) \longmapsto g \circ f$ により

$$\mathrm{Hom}(G, G') \times \mathrm{Hom}(G', G'') \longrightarrow \mathrm{Hom}(G, G'')$$

なる写像が得られる．$\mathrm{Hom}(G, G)$ をとくに $\mathrm{End}(G)$ と表す．

群 G から G 自身への同型写像を **自己同型** とよび，その全体を $\mathrm{Aut}(G)$ で表す．$\mathrm{Aut}(G)$ は写像の合成

$$(f \cdot g)(x) = f(g(x)) \qquad (f, g \in \mathrm{Aut}(G),\ x \in G)$$

を積として群をなす．これを **自己同型群** とよぶ．$a \in G$ とすると，

$$I_a : \quad G \ni x \longmapsto axa^{-1} \in G$$

なる写像は自己同型となる．この形の自己同型を **内部自己同型** といい，その全体を $\mathrm{Inn}(G)$ で表す．$\mathrm{Inn}(G)$ は $\mathrm{Aut}(G)$ の正規部分群をなし，商群 $\mathrm{Aut}(G)/\mathrm{Inn}(G)$ を $\mathrm{Out}(G)$ で表し，G の **外部自己同型群** とよぶ．

$$N \lhd G \iff I_a(N) = N \qquad (\forall a \in G)$$

であったが，これを強めて，G の部分群で，任意の G の自己同型で不変なものを **特性部分群** とよぶ．

群の準同型の列

$$\cdots \longrightarrow G_{i-1} \xrightarrow{f_i} G_i \xrightarrow{f_{i+1}} G_{i+1} \longrightarrow \cdots$$

において，$\mathrm{Im}(f_i)=\mathrm{Ker}(f_{i+1})$ が成り立つなら，この列は**完全(系)列**であるという．f： $G \longrightarrow G'$ を準同型とする．このとき上の言葉を使うと，

$$f\text{ が単射} \iff \{1\} \longrightarrow G \xrightarrow{f} G' \text{ が完全}$$

$$f\text{ が全射} \iff G \xrightarrow{f} G' \longrightarrow \{1\} \text{ が完全}$$

と表現できる．ここで $\{1\} \longrightarrow G$ および $G' \longrightarrow \{1\}$ なる準同型は一意的に定まるから略記した．したがって

$$f\text{ が同型} \iff \{1\} \longrightarrow G \xrightarrow{f} G' \longrightarrow \{1\} \text{ が完全}$$

となる．以下 $\{1\}$ を 1 と略記する．

N が G の正規部分群だとすると，自然な単射 i： $N \ni a \longmapsto a \in G$ と自然な準同型 π： $G \longrightarrow G/N$ が作れ，しかも $\mathrm{Im}(i)=N=\mathrm{Ker}(\pi)$ が成り立つ．よって

$$1 \longrightarrow N \xrightarrow{i} G \xrightarrow{\pi} G/N \longrightarrow 1$$

は完全列となる．逆に

$$1 \longrightarrow G' \xrightarrow{i} G \xrightarrow{\pi} G'' \longrightarrow 1$$

が完全列なら，$G' \simeq \mathrm{Im}(i) \lhd G$，$G/\mathrm{Im}(i) \simeq G''$ となる．この様な完全列を**短完全列**とよぶ．

短完全列 $1 \longrightarrow G' \xrightarrow{i} G \xrightarrow{\pi} G'' \longrightarrow 1$ において，G が G'' と同型な群 $\tilde{G}''$ を含み，かつ π が同型 $\tilde{G}'' \xrightarrow{\sim} G''$ を導くとき，この完全列は**分解**するという．これは j： $G'' \longrightarrow G$ なる準同型で $\pi \circ j = \mathrm{id}_{G''}$ なるものが存在することと同値である．また G が G' という正規部分群の他に，G'' という部分群で，$G' \cap G'' = \{1\}$，$G' \cdot G'' = G$ なるものを含むこととも同値である．この場合，G を G' の G'' による**半直積**とよび，また G は G'' の G' による**拡大**であるともいう．このとき $g=bc$ と $g'=b'c'$ $(b,b' \in G',\ c,c' \in G'')$ の積は

$$g \cdot g' = b(cb'c^{-1})cc'$$

で与えられる．つまり G' と G'' の成分ごとの積 $bb'cc'$ において，b' を $cb'c^{-1} \in G'$ でおき直したものとなっている．

問題 2. 8 (5–lemma) 群の可換図式

$$\begin{array}{ccccccccc}
G_1 & \xrightarrow{h_1} & G_2 & \xrightarrow{h_2} & G_3 & \xrightarrow{h_3} & G_4 & \xrightarrow{h_4} & G_5 \\
{\scriptstyle f_1}\downarrow & & {\scriptstyle f_2}\downarrow & & {\scriptstyle f_3}\downarrow & & {\scriptstyle f_4}\downarrow & & {\scriptstyle f_5}\downarrow \\
G_1' & \xrightarrow[h_1']{} & G_2' & \xrightarrow[h_2']{} & G_3' & \xrightarrow[h_3']{} & G_4' & \xrightarrow[h_4']{} & G_5'
\end{array}$$

において，横の列が完全で，f_1, f_2, f_4, f_5 が同型なら，f_3 も同型となることを示せ．

§3. 群の作用と置換表現

3. 1 群の作用 G を群，X を集合とし，写像 $f: G \times X \longrightarrow X$ が与えられたものとする．このとき，f による (a, x) $(a \in G,\ x \in X)$ の像 $f(a, x)$ を $a \cdot x$ と表す．この写像が次の性質をもつとき，群 G は集合 X に **作用** しているとよび，G を X 上の **変換群** とよぶ：

(TR 1) $(a \cdot b) \cdot x = a \cdot (b \cdot x)$ $(\forall a, b \in G,\ \forall x \in X)$,

(TR 2) $1 \cdot x = x$ $(\forall x \in X)$.

第Ⅰ章，§4 では作用の定義に (**TR 1**) のみを仮定したが，いまは G が群であり単位元 1 を含むので (**TR 2**) も仮定する．

G を X 上の変換群とする．このとき

$$t_a: \quad X \ni x \longmapsto a \cdot x \in X \qquad (a \in G)$$

は，$t_{a^{-1}} \circ t_a = t_a \circ t_{a^{-1}} = t_1 = \mathrm{id}_X$ を満たすから，X から X 自身への全単射を与える．よって t_a は X 上の置換群 $S(X)$（Ⅰ，例 5.6 参照）の元である．また

$$t_{ab}(x) = (ab)(x) = a(bx) = t_a(t_b(x))$$

が成り立つから，

$$t: \quad G \ni a \longmapsto t_a \in S(X)$$

は群の準同型となる．これを G の X 上での **置換表現** とよぶ．

逆に $t:\ G \longrightarrow S(X)$ を群の準同型とすると，

$$G \times X \ni (a, x) \quad \longmapsto \quad t(a)(x) \in X$$

により，群 G は集合 X の上に作用する．

群 G が集合 X に作用しているものとする．このとき，G の X 上での置換表現が単射となるなら，この作用は **忠実** である，または **効果的** であるという．これは

$$a \neq 1 \quad \Longrightarrow \quad \text{ある } x \in X \text{ に対し } ax \neq x$$

を意味する．

X の2元 x, y は，ある $a \in G$ があり $ax = y$ となるとき **G-同値** であるといい $x \underset{G}{\sim} y$ と表す．X をこの同値関係により類別した各同値類を **G-軌道** とよび，その全体を $G\backslash X$ で表す．X 自身が1つの軌道をなすとき，この G の X への作用は **推移的** であるという．

G を X 上の変換群とするとき，$x \in X$ に対し

$$G_x = \{a \in G \mid ax = x\}$$

とおき，x における G の **等方部分群** とよぶ．$gx = y$ なら $G_y = gG_xg^{-1}$ となるから，同じ G-軌道に属する点での等方部分群は互いに同型である．

定理 3.1 G を有限群とし，G が X 上に作用しているとする．$x \in X$ に対し，x を通る軌道 Gx の含む元の個数 $|Gx|$ は，$[G : G_x]$ に等しい．

[証明] G_x は G の部分群であるから，G の G_x による左剰余類への分類が考えられる．このとき，

$$aG_x = bG_x \iff ax = bx$$

が成り立つ．よって，左剰余類の個数 $|G/G_x| = [G : G_x]$ は，x を含む G 軌道 Gx が含む元の個数 $|Gx|$ に等しい． (証明終)

例 3.2 G を群，H を G の部分群とする．このとき H は G の上に，

$$H \times G \ni (h, a) \quad \longmapsto \quad h \cdot a \in G$$

で作用する．この作用に関する H-軌道は，G の部分群 H による右剰余類を与える．こ

の意味で，G の H による右剰余類への分解は，G の H–軌道への分解 $H\backslash G$ の特別な場合と思える．

3. 2 共役類 G を群とし，G を G 自身の上へ内部自己同型で作用させる：

$$G \times G \ni (a, x) \longmapsto I_a(x) = axa^{-1} \in G.$$

これにより，G は G 自身の上の変換群となる．

G の 2 元 x, y は，ある $a \in G$ があり

$$y = axa^{-1}$$

となるとき **共役** であるという．これは上の G の作用により，x, y が同じ G–軌道に属することを意味する．この場合，x を含む G–軌道を x の **共役類** とよぶ．$x \in G$ における等方部分群は $C_G(x) = \{a \in G \mid ax = xa\}$ となる．これを x における G の **中心化群** とよぶ．

G が有限群であるものとし，$C_1, C_2, \cdots, C_l$ をその共役類の全体とする．$|C_i| = 1$ となるのは，$C_i = \{x_i\}$ $(x_i \in Z(G))$ のときに限るから，$G = \coprod C_i$ の両辺の元の個数を比較すると，

$$|G| = |Z(G)| + \sum_{|C_i|>1} |C_i|$$

が成り立つことがわかる．これを **類等式** とよぶ．定理 3.1 より $|C_i| = [G : C_G(x)]$ であり，これは G の位数の約数である．

X を G の部分集合の全体，Y を G の部分群の全体とし，X と Y に G を内部自己同型で作用させる．このとき $S \in X$ での等方部分群は，

$$N_G(S) = \{a \in G \mid aSa^{-1} = S\}$$

である．これを S の **正規化群** とよぶ．$N_G(S)$ は S の **中心化群**

$$C_G(S) = \{a \in G \mid as = sa \ (\forall s \in S)\}$$

を含む．G の部分群 H_1, H_2 は，G の Y へのこの作用により G–同値となるとき，**共役** であるという．これにより，G の部分群の共役部分群への類別が得られる．

3.3 対称群 S_n を集合 $\Omega = \{1, 2, \cdots, n\}$ 上の全単射な写像全体のなす群（n 次対称群）とする．このとき S_n は Ω 上の変換群となり，S_n は Ω 上に忠実かつ推移的に作用する．

σ を S_n の元とし，$i_1 \in \Omega$ とする．r を $\sigma^r(i_1) = i_1$ となる最小の自然数とし，$\sigma(i_1) = i_2$, $\sigma(i_2) = i_3, \cdots, \sigma(i_{r-1}) = i_r$ とすると，$i_1, i_2, \cdots, i_r$ は互いに相異なる Ω の元で，$\sigma(i_r) = i_1$ となる．$i_1, i_2, \cdots, i_r$ をこのように巡回的に動かし，他の Ω の元は動かさぬ Ω から Ω への写像を $(i_1, i_2, \cdots, i_r)$ で表すと，これは S_n の元を与える．このような S_n の元を長さ r の **巡回置換** とよぶ．$(i_1, i_2, \cdots, i_r)$ を上のようにとると，$(i_1, i_2, \cdots, i_r)^{-1}\sigma$ は $\{i_1, i_2, \cdots, i_r\} \subset \Omega$ を動かさず，それ以外の Ω の元に対しては σ と同じ作用をする．そこで $\Omega \setminus \{i_1, i_2, \cdots, i_r\}$ から任意の 1 元をとり出し同じことを繰り返す．このことを，σ がすべての Ω の元を固定するようになるまで繰り返すことにより，次の定理が得られる．

定理 3.3 n 次対称群 S_n の任意の元は，互いに共通する文字を含まないいくつかの巡回置換の積として，順序の差を除き一意的に表される．

［証明］ 表現の可能性は既に示した．一意性は，このような巡回置換の積として書けるなら，これら巡回置換は上の様な性質をもつことをみればよい． （証明終）

問題 3.4 S_n の元 σ を定理の様に分解したとき，長さ r の巡回置換がちょうど m_r 個現れたとする．このとき σ の **型** は $1^{m_1}\, 2^{m_2} \cdots n^{m_n}$ であるという．S_n の 2 元が共役となるための必要十分条件は，この型が一致することである．

とくに 2 つの元の巡回置換を **互換** という．等式

$$(i_1, i_2, \cdots, i_r) = (i_1\ i_r)\,(i_1, i_2, \cdots, i_{r-1}) = (i_1\ i_r) \cdots (i_1\ i_3)\,(i_1\ i_2)$$

が成り立つから，定理 3.3 より次の定理が導かれる．

定理 3.5 n 次対称群 S_n の任意の元は，いくつかの互換の積として表される．

問題 3.6 n 次対称群 S_n は，$\{(1\ 2), (2\ 3), \cdots, (n-1\ n)\}$ により生成されることを

示せ.

$\sigma \in S_n$ の符号 $\mathrm{sgn}(\sigma)$ を第Ⅰ章，例5.6のように

$$\prod_{i<j} (x_{\sigma(i)} - x_{\sigma(j)}) = \mathrm{sgn}(\sigma) \prod_{i<j} (x_i - x_j)$$

で定める．σ が互換のときは，$\mathrm{sgn}(\sigma) = -1$ となることが容易にわかる．一般に，$\sigma \in S_n$ が m 個の互換の積として表されたとすると，$\mathrm{sgn}(\sigma) = (-1)^m$ となる．$\mathrm{sgn}(\sigma) = 1$ のとき σ を **偶置換**，$\mathrm{sgn}(\sigma) = -1$ のとき σ を **奇置換** とよぶ．

$\mathrm{sgn}(\sigma)$ の定義より

$$\mathrm{sgn}(\tau\sigma) = \mathrm{sgn}(\tau)\,\mathrm{sgn}(\sigma)$$

が成り立つから，$\mathrm{sgn}:\ S_n \longrightarrow \{\pm 1\}$ は，群 S_n から ± 1 のなす乗法群への準同型写像である．この写像の核を，n 次 **交代群** とよび A_n で表す．$n \geqq 2$ なら S_n は互換を含み，準同型 sgn は全射となる．よって，準同型定理より $A_n \lhd S_n$，$S_n/A_n \simeq \{\pm 1\}$ となる．

S_n の $n \in \Omega$ での固定群は，$\{1, 2, \cdots, n-1\}$ からそれ自身への全単射の全体とみなせるから，S_{n-1} と同一視できる．S_n は $\Omega = \{1, 2, \cdots, n\}$ の上に推移的に作用するから，定理 3.1 より，$[S_n : S_{n-1}] = n$ となる．よって帰納法で

$$|S_n| = n\,!$$

となることがわかる．

§4. シローの定理

位数が素数 p のべきの有限群を **p-群** といい，G が位数 $p^n m$（p は素数，m は p と素な整数）の有限群のとき，位数が p^n の G の部分群を **シロー p-部分群** とよぶ．次にのべるシローの定理は，有限群の構造を調べるときの基本的手段となる，非常に重要な定理である．

定理 4.1 (シロー) Gを有限群とする．このとき，

(1) HをGのp-部分群 ($H=\{1\}$ でもよい) とすると，Hを含むGのシローp-部分群が存在する．

(2) シローp-部分群はすべて互いに共役である．

(3) シローp-部分群の個数は $kp+1$ (kは整数) の形である．

[証明] まずシローp-部分群が存在することを示す．$|G|=g=p^n m$, $(m,p)=1$ とする．$n=0$ のときは明らかだから $n\geqq 1$ とする．Gの部分集合Sで，$|S|=p^n$ となるものの全体をXとし，GのXへの作用を

$$G\times X\ni(a,S)\longmapsto aS=\{as\mid s\in S\}\in X$$

で定義する．Xの元の個数$|X|$は，g個からp^n個を選ぶ組み合わせの個数$\binom{g}{p^n}$で与えられる．$g=p^n m$ であるから

$$\binom{g}{p^n}=\frac{p^n m(p^n m-1)(p^n m-2)\cdots(p^n m-p^n+1)}{p^n(p^n-1)(p^n-2)\cdots 1}$$

である．$n\geqq 1$だから，$p^n m-i\equiv p^n-i \pmod{p^n}$ より，$p^n m-i$ と p^n-i $(1\leqq i\leqq p^n-1)$ はpの同じべきで割り切れる．よって$\binom{g}{p^n}$とmは同じpのべきで割り切れる．ところが，mはpと素だから，$|X|$もpと素となる．よってXのG-軌道GSで，その元の個数がpと素なものが存在する．

PをSの等方部分群とする．このとき，定理3.1より $[G:P]=|GS|$ はpと素となる．ところが $|G|=[G:P]|P|$ であるから，p^nはPの位数 $|P|$ を割り切る．他方 $PS=S$ であるから，$s\in S$ をとると $Ps\subset S$ となり，$|P|\leqq|S|=p^n$ となる．よって $|P|=p^n$ となり，Pはシローp-部分群となる．

PをGのシローp-部分群とし，YでPと共役なGの部分群全体の集合を表す．HをGのp-部分群とし，HをYの上に内部自己同型写像で作用させ，YをH-軌道に分ける．定理3.1より，Yの各H-軌道の含む元の個数は$|H|$の約数であり，pのべきである．他方 $P\subset N_G(P)$ であるから，$|Y|=[G:N_G(P)]$ は $[G:P]$ の約数であり，pとは素である．したがってあるYのH-軌道は $p^0=1$ 個の元から成る．いい直すと，ある $P'\in Y$ でHで固定されるものが存在する．このとき $H\subset N_G(P')$ であるから，$HP'=P'H$ となり，問題1.4によりHP'はGの部分群となる．また $P'\lhd HP'$ であるから，同型定理により $H/P'\cap H\simeq HP'/P'$ となる．よって $|HP'|\cdot|P'\cap H|=|H|\cdot|P'|$ はpべきとなり，$|HP'|$ はpべきとなる．ところが $P'\subset HP'\subset G$ にお

いて，$|P'|$ は $|G|$ を割る最大の p べきであるから，$|HP'|=|P'|$ となり，$HP'=P'$ となる．いい直すと，$H\subset P'$ であり，これで（1）が証明された．

とくに H 自身がシロー p-部分群なら，以上の議論より $H=P'\in Y$ となり，H は P と共役となる．またこれより，Y が G のシロー p-部分群の全体と一致することもわかる．

さらに以上の議論より，$P'\in Y$ を含む H-軌道が唯一つの元から成るなら，$P'=H$ となることもわかった．したがってこの様な H-軌道は唯一つしかなく，他の H-軌道は p の倍数個の元を含む．よって $|Y|\equiv 1 \pmod p$ となり，(3) も成り立つ．（証明終）

例 4．2 p,q を $p>q$ なる素数とし，G を位数 pq の有限群とする．このときシローの定理より，G はシロー p-部分群 P を含む．$G\supset N_G(P)\supset P$ かつ $[G:P]=q$ は素数であるから，$N_G(P)=G$ または $N_G(P)=P$ となる．ところが，シローの定理より，P と共役な G の部分群の個数 $[G:N_G(P)]$ は $kp+1$ の形であり，1 でなければ p より大である．よって $[G:N_G(P)]=1$ だから，$N_G(P)=G$ となり，P は G の正規部分群となる．

G のシロー q-部分群を Q とする．$P\lhd G$ より PQ は G の部分群となり，位数が pq の倍数だから，$PQ=G$ となる．また位数の関係より $P\cap Q=\{1\}$ となるから，G は P の Q による半直積となる．

$P\lhd G$ だから，Q は P に内部自己同型写像で作用している．ところが $P\simeq \boldsymbol{Z}/p\boldsymbol{Z}$ であるから，$\mathrm{Aut}(P)$ は位数 $p-1$ の群である．したがって，q が $p-1$ を割り切らないなら，$\mathrm{Aut}(P)$ の部分群で Q の準同型像となり得るのは $\{1\}$ のみである．したがって，$q\nmid(p-1)$ なら Q は P の上に自明に（id_P として）作用し，P の元と Q の元は可換となる．よって，$q\nmid(p-1)$ なら $G=PQ$ は位数 pq のアーベル群となる．（次の §5 の結果を使えば，この様な群 G は巡回群となることもわかる．）

§5. 直　積

H_1,H_2 を群とし，G を集合 H_1 と H_2 の直積とする：

$$G=\{a=(a_1,a_2)\mid a_1\in H_1,\ a_2\in H_2\}.$$

G の元 $a=(a_1,a_2)$ と $b=(b_1,b_2)$ の積を 成分ごとの積

$$a\cdot b=(a_1\cdot b_1,\ a_2\cdot b_2)$$

で定義する．H_1, H_2 では結合法則が成り立つから，このようにして定義した G の積も結合法則を満たす．またこの積に関し，$1=(1,1)$ が G の単位元となり，$a=(a_1,a_2)$ の逆元が $a^{-1}=(a_1{}^{-1},a_2{}^{-1})$ で与えられることも明らかである．よって G は群となる．これを群 H_1 と H_2 の **直積** とよぶ．

G を群 H_1, H_2 の直積とすると，

$$H_1 \ni a_1 \longmapsto (a_1,1) \in G, \qquad H_2 \ni a_2 \longmapsto (1,a_2) \in G$$

は H_1, H_2 より G の中への単射な準同型であるから，これにより H_1, H_2 を G の部分群と思える．このとき，H_1 の元 $(a_1,1)$ と H_2 の元 $(1,a_2)$ とは可換であり，G の任意の元 $a=(a_1,a_2)$ は H_1 の元 $(a_1,1)$ と H_2 の元 $(1,a_2)$ との積に一意的に表される．次の定理により，この逆が成り立つ．

定理 5.1 H_1, H_2 を群 G の部分群とする．もし次の2条件が成り立つなら，$G \simeq H_1 \times H_2$ となる：

（1） H_1 の元と H_2 の元は可換である．

（2） G の任意の元は，H_1 の元と H_2 の元の積として一意的に表される．

[証明]

$$f:\ H_1 \times H_2 \ni (a_1,a_2) \longmapsto a_1 \cdot a_2 \in G$$

なる写像を考える．これは仮定（1）より準同型写像となる．また仮定（2）より f は全単射になる．（証明終）

以下この定理の条件を満たすとき，G は部分群 H_1 と H_2 の **直積** であるということにする．

定理 5.2 H_1, H_2 を群 G の部分群とする．このとき，G が H_1 と H_2 の直積となるための必要十分条件は，次の3条件が満たされることである：

（a） H_1, H_2 は G の正規部分群である．

（b） $G = H_1H_2$．

（c） $H_1 \cap H_2 = \{1\}$．

[証明] （必要性）　$G = H_1 \times H_2$ とする．このとき，定理5.1の前に注意したように，G の任意の元 a は，$a = a_1 \cdot a_2$ $(a_1 \in H_1,\ a_2 \in H_2)$ と一意的に書けるから，(b)，(c) が成り立つ．また H_1 の元と H_2 の元は可換だから，$b_1 \in H_1$，$b_2 \in H_2$ をとると，

任意の G の元 $a=a_1\cdot a_2$ $(a_1\in H_1,\ a_2\in H_2)$ に対し，

$$ab_1a^{-1}=a_1b_1a_1^{-1}\in H_1,\qquad ab_2a^{-1}=a_2b_2a_2^{-1}\in H_2$$

となる．よって $H_1, H_2\lhd G$ となり，(a) が成り立つ．

（十分性）　(a),(b),(c) を仮定する．(b) より G の任意の元 a は，$a=a_1\cdot a_2$ $(a_1\in H_1,\ a_2\in H_2)$ と書ける．また $a=b_1\cdot b_2$ $(b_1\in H_1,\ b_2\in H_2)$ とも書けたとすると，$a_1^{-1}b_1=a_2b_2^{-1}\in H_1\cap H_2$ となるから，(c) より $a_1=b_1$，$a_2=b_2$ となり，前定理の (2) が成り立つ．そこで $c_1\in H_1$，$c_2\in H_2$ を任意にとってくる．このとき (a) より H_1，$H_2\lhd G$ が成り立つから，$c_1c_2c_1^{-1}c_2^{-1}$ は $c_1\cdot(c_2c_1^{-1}c_2^{-1})$ と変形することにより H_1 の元となり，$(c_1c_2c_1^{-1})\cdot c_2$ と変形することにより H_2 の元となることがわかる．ところが $H_1\cap H_2=\{1\}$ であるから

$$c_1c_2c_1^{-1}c_2^{-1}=1 \iff c_1c_2=c_2c_1$$

が成り立ち，H_1 の元と H_2 の元は可換となり，(1) も成り立つ．　（証明終）

（注）　定理 5.2 より，群 G が部分群 H_1 と H_2 の直積であるとは，「G は H_1 の H_2 による半直積で，H_1 の上に H_2 を内部自己同型で作用させたとき，その作用が自明になるもの」という形でも表現できることがわかる．

$H_1, H_2, \cdots, H_n$ を有限個の群とするとき，これらの直積 $H_1\times H_2\times\cdots\times H_n$ も帰納的に定義できる．

問題 5.3　群 G の部分群 $H_1, H_2, \cdots, H_n$ が次の 2 条件を満たすなら $G\simeq H_1\times H_2\times\cdots\times H_n$ となることを示せ：

(1)　$i\neq j$ なら H_i と H_j の元は可換である．

(2)　G の任意の元 a は，$a=a_1\cdot a_2\cdot\cdots\cdot a_n$ $(a_i\in H_i)$ と一意的に表される．

また，この 2 条件は次の 3 条件とも同値であることを示せ．

(a)　$H_i\lhd G$　$(i=1,2,\cdots,n)$．

(b)　$G=H_1\cdot H_2\cdot\cdots\cdot H_n$．

(c)　$(H_1\cdot H_2\cdot\cdots\cdot H_{i-1})\cap H_i=\{1\}$　$(i=2,3,\cdots,n)$．

群 G の部分群 H は，適当な部分群 K をとると $G=H\times K$ となるとき，G の **直積因子** であるという．G が G 自身 および $\{1\}$ 以外に直積因子をもた

ないなら，G は**直既約**であるという．

命題5.4 $G=\boldsymbol{Z}/m\boldsymbol{Z}$（$m$ は自然数）とおく．このとき，

（1） $m=m_1m_2$（m_1, m_2 は互いに素）なら $G\simeq(\boldsymbol{Z}/m_1\boldsymbol{Z})\times(\boldsymbol{Z}/m_2\boldsymbol{Z})$ となる．

（2） m が素数のべき p^n なら，G は直既約である．

［証明］（1） $f:\ \boldsymbol{Z}\ni a \longmapsto (a(\mathrm{mod}\, m_1), a(\mathrm{mod}\, m_2))\in(\boldsymbol{Z}/m_1\boldsymbol{Z})\times(\boldsymbol{Z}/m_2\boldsymbol{Z})$ なる準同型写像を考える．$(m_1, m_2)=1$ であるから，この写像の核は $m_1\boldsymbol{Z}\cap m_2\boldsymbol{Z}=m_1m_2\boldsymbol{Z}=m\boldsymbol{Z}$ である．よって準同型定理より $\boldsymbol{Z}/m\boldsymbol{Z}\simeq\mathrm{Im}(f)$ となる．ところが $\mathrm{Im}(f)\subset(\boldsymbol{Z}/m_1\boldsymbol{Z})\times(\boldsymbol{Z}/m_2\boldsymbol{Z})$ より，$|\mathrm{Im}(f)|\leqq|(\boldsymbol{Z}/m_1\boldsymbol{Z})\times(\boldsymbol{Z}/m_2\boldsymbol{Z})|=m_1m_2=m$ である．よって $|\mathrm{Im}(f)|=|\boldsymbol{Z}/m\boldsymbol{Z}|=m=|(\boldsymbol{Z}/m_1\boldsymbol{Z})\times(\boldsymbol{Z}/m_2\boldsymbol{Z})|$ であるから，$\mathrm{Im}(f)=(\boldsymbol{Z}/m_1\boldsymbol{Z})\times(\boldsymbol{Z}/m_2\boldsymbol{Z})$ となり，$\boldsymbol{Z}/m\boldsymbol{Z}\simeq(\boldsymbol{Z}/m_1\boldsymbol{Z})\times(\boldsymbol{Z}/m_2\boldsymbol{Z})$ となる．

（2） $m=p^n$ とし，$\boldsymbol{Z}/m\boldsymbol{Z}=A\times B$, $A, B\neq\{1\}$ とする．このとき，A, B はそれぞれ位数 p の部分群 A_1, B_1 を含む．$A\cap B=\{1\}$ より $A_1\neq B_1$ であるが，これは巡回群 $\boldsymbol{Z}/m\boldsymbol{Z}$ が位数 p の部分群を2つもつことになり，矛盾である（例2.6を参照せよ）．

（証明終）

§6. 有限アーベル群

この節では有限アーベル群の構造を調べる．この結果は有限生成アーベル群の場合に拡張できるが，その拡張は単因子の理論の応用として第Ⅳ章でのべる．また本節ではアーベル群のみを扱うので，乗法でなく加法の形で書く．

定理6.1 G を有限アーベル群とすると，G は

$$G\simeq(\boldsymbol{Z}/{p_1}^{e_1}\boldsymbol{Z})\times(\boldsymbol{Z}/{p_2}^{e_2}\boldsymbol{Z})\times\cdots\times(\boldsymbol{Z}/{p_t}^{e_t}\boldsymbol{Z})$$

（$p_1, p_2, \cdots, p_t$ は素数，$e_1, e_2, \cdots, e_t$ は自然数）と，素数べき位数の巡回群の直積に書ける．しかも，G をこのような形に表現するとき，$\{{p_1}^{e_1}, {p_2}^{e_2}, \cdots, {p_t}^{e_t}\}$ は順序の差を除き一意的に定まる．

［証明］ G の位数を g とし，g を割る素数 p をとり，$g=qh$, q は p のべき，$(p,h)=1$ と表す．P で位数が q の約数である G の元全体のなす集合，H で位数が h の約数である G の元全体のなす集合を表す．G はアーベル群で，q,h は G の位数の約数だから，P と H は G の部分群となる．$(q,h)=1$ だから $sq+th=1$ となる整数 s,t が存在する．このとき $\forall a\in G$ は，

$$a=1\cdot a=sqa+tha$$

と書ける．ところが

$$h(sqa)=g(sa)=0, \qquad q(tha)=g(ta)=0$$

となるから，$sqa\in H$, $tha\in P$ となり，$G=P+H$ が成り立つ．また $P\cap H$ の元は，位数が q の約数でも h の約数でもあるから，$(q,h)=1$ より $P\cap H=\{0\}$ となる．さらに，G はアーベル群だから，P,H は G の正規部分群となる．よって定理 5.2 より $G=P\times H$ と直積になる．P は G の位数が p べきの部分群をすべて含み，H は位数が p と素な部分群をすべて含む．よって G が p–群のとき定理を証明すれば十分である．

G が p–群であるとし，$g=|G|$ に関する帰納法で直積分解できることを示す．a を G の位数最大の元とし，$\langle a\rangle$ が G の直積因子となることを，g に関する帰納法で示す．$G=\langle a\rangle$ なら明らかだから，$\langle a\rangle \subsetneqq G$ とし，G の元 b で $b\notin\langle a\rangle$, $pb\in\langle a\rangle$ となるものをとる．$pb\in\langle a\rangle$ より $pb=ma$ $(m\in \boldsymbol{Z})$ と書けるが，$(m,p)=1$ なら $pb=ma$ が $\langle a\rangle$ を生成し，b の位数 $o(b)=po(a)>o(a)$ となり，a のとり方に矛盾する．よって $m=pm'$ $(m'\in\boldsymbol{Z})$ と書ける．そこで $c=b-m'a$ とおく．$b\notin\langle a\rangle$ より $c\neq 0$, また $pc=0$ である．c の位数は素数であるから，$\langle c\rangle$ の 0 以外の元は $\langle c\rangle$ を生成する．ところが $c\notin\langle a\rangle$ だから $\langle a\rangle\cap\langle c\rangle=\{0\}$ となる．したがって，自然準同型 $\pi: G\longrightarrow G/\langle c\rangle$ を考えると，$\langle a\rangle\simeq\langle\pi(a)\rangle$ となる．a は G の位数最大の元であるから，それと同じ位数をもつ $\pi(a)$ は $G/\langle c\rangle$ の位数最大の元となる．よって帰納法の仮定より，

$$\pi(G)=\langle\pi(a)\rangle\times Q'$$

と直積分解できる．$\pi^{-1}(Q')=Q$ とおくと，$Q\supset\langle c\rangle$ が成り立つ．$\langle\pi(a)\rangle+Q'=\pi(G)$, $Q\supset\langle c\rangle=\mathrm{Ker}(\pi)$ だから，準同型定理より $\langle a\rangle+Q=G$ となる．また $\langle\pi(a)\rangle\cap Q'=\{0\}$ より $\langle a\rangle\cap Q\subset\mathrm{Ker}(\pi)=\langle c\rangle$ となり，$\langle a\rangle\cap Q\subset\langle a\rangle\cap\langle c\rangle=\{0\}$ となる．よって，定理 5.2 より $G=\langle a\rangle\times Q$ と直積になる．Q も p 群で $|Q|<|G|$ であるから，帰納法の仮定より，Q は位数が p べきの巡回群の直積に書ける．$\langle a\rangle$ も位数が p べきの巡回群だから，定理の直積分解の存在がいえた．

一意性も $g = |G|$ に関する帰納法でいう.

$$G \simeq (\boldsymbol{Z}/p^{e_1}\boldsymbol{Z}) \times (\boldsymbol{Z}/p^{e_2}\boldsymbol{Z}) \times \cdots \times (\boldsymbol{Z}/p^{e_t}\boldsymbol{Z})$$

$(e_1 = e_2 = \cdots = e_s > e_{s+1} \geqq e_{s+2} \geqq \cdots \geqq e_t)$ とし，$e = e_1$,

$$G^* = \{a \in G \mid a \text{ の位数は高々 } p^{e-1}\}$$

とおく．このとき G^* は G の直積因子のうち，$\boldsymbol{Z}/p^e\boldsymbol{Z}$ なるものを $\boldsymbol{Z}/p^{e-1}\boldsymbol{Z}$ でおき換えたものとなる．よって帰納法の仮定より，G^* に対する不変量の組である $\{p_1{}^{e-1}, p_2{}^{e-1}, \cdots, p_s{}^{e-1}, p_{s+1}{}^{e_{s+1}}, p_{s+2}{}^{e_{s+2}}, \cdots, p_t{}^{e_t}\}$ が定まる．他方

$$G/G^* \simeq (\boldsymbol{Z}/p\boldsymbol{Z}) \times \cdots \times (\boldsymbol{Z}/p\boldsymbol{Z}) \qquad (s \text{ 個の直積})$$

であるから，s も定まる．よって，G より $\{p_1{}^{e_1}, p_2{}^{e_2}, \cdots, p_s{}^{e_s}, p_{s+1}{}^{e_{s+1}}, p_{s+2}{}^{e_{s+2}}, \cdots, p_t{}^{e_t}\}$ が一意的に定まる．　　　　（証明終）

定理 6.1 と命題 5.4 をあわせると，次の様にも表現できる．

定理 6.2　G を有限アーベル群とすると，整数 $e_1, e_2, \cdots, e_t \geqq 2$ があり，

$$G \simeq (\boldsymbol{Z}/e_1\boldsymbol{Z}) \times (\boldsymbol{Z}/e_2\boldsymbol{Z}) \times \cdots \times (\boldsymbol{Z}/e_t\boldsymbol{Z})$$

$$e_i | e_{i+1} \qquad (i = 1, 2, \cdots, t-1)$$

と直積分解できる．しかも $\{e_1, e_2, \cdots, e_t\}$ なる集合は G により一意的に定まる．

例 6.3　p を素数とすると，位数が p^4 の群は，

$$G_1 = (\boldsymbol{Z}/p^4\boldsymbol{Z}), \quad G_2 = (\boldsymbol{Z}/p^3\boldsymbol{Z}) \times (\boldsymbol{Z}/p\boldsymbol{Z}), \quad G_3 = (\boldsymbol{Z}/p^2\boldsymbol{Z}) \times (\boldsymbol{Z}/p^2\boldsymbol{Z})$$

$$G_4 = (\boldsymbol{Z}/p^2\boldsymbol{Z}) \times (\boldsymbol{Z}/p\boldsymbol{Z}) \times (\boldsymbol{Z}/p\boldsymbol{Z}),$$

$$G_5 = (\boldsymbol{Z}/p\boldsymbol{Z}) \times (\boldsymbol{Z}/p\boldsymbol{Z}) \times (\boldsymbol{Z}/p\boldsymbol{Z}) \times (\boldsymbol{Z}/p\boldsymbol{Z})$$

の 5 個がある．これらの群の位数が p となる元の個数は，それぞれ $p-1$, p^2-1, p^2-1, p^3-1, p^4-1 である．また位数が p^2 の元の個数は，それぞれ p^2-p, p^3-p^2, p^4-p^2, p^4-p^3, 0 である．よってこれらの群は互いに同型ではない．

問題 6.4　位数 g の有限アーベル群が巡回群となるためには，任意の g の約数 n に対し，$nx = 0$ となる G の元が高々 n 個しかないことが必要十分であることを示せ．（もちろん，G が巡回群となるなら，$\#\{x \in G \mid nx = 0\} = n$ となる．アーベル群という仮定はなくてもよいが，そうすると証明は大分難しくなる．）

§7. 作用域をもつ群

集合 Λ の群 G への作用 $\Lambda \times G \longrightarrow G$ が定められ,

$$\lambda(a \cdot b) = (\lambda a) \cdot (\lambda b) \qquad (\lambda \in \Lambda,\ a, b \in G)$$

が成り立つとき, G は **作用域 Λ をもつ群**, または簡単に **Λ-群** とよぶ. 例えば, R を環とし, M を左 R-加群とすると, M は作用域 R をもつアーベル群となる.

G を Λ-群, $\lambda \in \Lambda$ とすると, 定義より

$$G \ni a \longmapsto \lambda \cdot a \in G$$

は群の準同型写像を与える. よって $\lambda 1 = 1$, $\lambda a^{-1} = (\lambda a)^{-1}$ などが成り立つ.

Λ-群 G の部分群 H は

$$\lambda \in \Lambda,\ h \in H \implies \lambda h \in H$$

が成り立つとき, **Λ-部分群** であるという. G を Λ-群, S を G の部分集合とするとき, S を含む G の最小の Λ-部分群を, S で生成される G の Λ-部分群とよぶ. また Λ-部分群が正規部分群とも成るとき, **Λ-正規部分群** であるという. Λ-群 G において G と $\{1\}$ は常に Λ-正規部分群となるが, 逆に Λ-群 G の Λ-正規部分群が G と $\{1\}$ に限るなら, G を **Λ-既約** または **Λ-単純** であるという.

G, G' が Λ-群のとき, f: $G \longrightarrow G'$ なる群の準同型写像は

$$f(\lambda a) = \lambda f(a) \qquad (\lambda \in \Lambda,\ a \in G)$$

を満たすとき, **Λ-準同型写像** であるといい, G から G' への Λ-準同型写像の全体を $\mathrm{Hom}_\Lambda(G, G')$ で表す. $f \in \mathrm{Hom}_\Lambda(G, G')$ なら $\mathrm{Im}(f)$ や $\mathrm{Ker}(f)$ は Λ-部分群となる.

準同型定理の証明と同様にして, Λ-群に対する準同型定理が証明できる:

定理 7.1 G, G' を Λ-群とし, f: $G \longrightarrow G'$ を Λ-準同型写像とする.

このとき $a\mathrm{Ker}(f) \longmapsto f(a)$ なる対応により

$$G/\mathrm{Ker}(f) \simeq \mathrm{Im}(f)$$

なる Λ-同型が得られる．さらに $H = f^{-1}(H') \longleftrightarrow H' = f(H)$ なる対応により，G の $\mathrm{Ker}(f)$ を含む Λ-部分群 H と，$\mathrm{Im}(f)$ の Λ-部分群 H' とが1対1に対応する．

準同型定理の系である同型定理なども，Λ-群に対して成り立つ．また Λ-群の直積は Λ-群であり，§5の結果も Λ-群に対して成り立つ．

例 7.2 G を群とし，内部自己同型群 $\mathrm{Inn}(G)$ を G に作用させる．このとき $\mathrm{Inn}(G)$-部分群とは，G の正規部分群のことをいう．

§8. 正 規 列

この節では作用域をもつ群の正規列についてのべるが，R が環で M が左（右）R-加群のときは，M は作用域 R をもつアーベル群となるから，この節の結果のうち8.1と8.2の結果は，左（右）R-加群に対しても成り立つ．実際8.1の結果などは，左（右）R-加群に対する場合が最も重要である．

8.1 有限性条件 Λ-群 G は，次の命題の3つの条件 (a), (b), (c) を満たすとき，(Λ-群として) **ネター的**であるという．

命題 8.1 作用域 Λ をもつ群について，以下は同値である．

(a) **(極大条件)** G の Λ-部分群の作る任意の空でない集合は，包含関係に関して極大元をもつ．

(b) **(昇鎖律)** $G_1 \subset G_2 \subset \cdots \subset G_n \subset \cdots$

を G の Λ-部分群の無限列とすると，ある番号 N より等号 $G_N = G_{N+1} = \cdots$ となる．

(c) **(基底律)** G の任意の Λ-部分群は，Λ-群として有限個の元より生

成される.

[証明] (a)$\Longrightarrow$(c). H を G の Λ-部分群とし, H の Λ-部分群で Λ-群として有限生成なもの全体を $\mathscr{H}$ で表す. $\mathscr{H}$ は $\{1\}$ を含むから空ではない. よって仮定 (a) より, $\mathscr{H}$ は極大元 H' をもつ. $H' \subsetneqq H$ なら, $a \in H$, $a \notin H'$ なる元をとり H' と a で生成される Λ-群を H'' とすると, $H' \subsetneqq H''$ かつ $H'' \in \mathscr{H}$ となり, H' のとり方に矛盾する. よって $H' = H$ となるから, H は Λ-群として有限生成となる.

(c) $\Longrightarrow$ (b). $G_1 \subset G_2 \subset \cdots \subset G_n \subset \cdots$ を Λ-部分群の列とし, $G' = \bigcup_{n \geqq 1} G_n$ とおく. G' は G の Λ-部分群となるから, 仮定 (c) より, 有限個の元 $a_1, a_2, \cdots, a_M$ により Λ-群として生成される. 各 a_i は G' の元だから, ある n_i に関し $a_i \in G_{n_i}$ となる. そこで $N = \max(n_1, n_2, \cdots, n_M)$ とおけば, $a_1, a_2, \cdots, a_M \in G_N$ となるから, $G' \subset G_N$ となる. よって $G_{N+j} \subset G' \subset G_N$ $(j \geqq 0)$ だから $G_N = G_{N+1} = \cdots$ となる.

(b) $\Longrightarrow$ (a). $\mathscr{M}$ を G の Λ-部分群の空でない集合とし, 包含関係により順序を入れる. $\mathscr{M}$ が帰納的順序集合となるなら, ツォルンの補題 (I, 定理 3.4) により極大元をもつ. $\mathscr{M}$ が帰納的でないとして矛盾を導く. よって $\mathscr{M}$ の全順序部分集合 $\mathscr{L}$ で上界をもたぬものが存在したとする. $G_1 \in \mathscr{L}$ を任意にとると, G_1 は $\mathscr{L}$ の上界ではないから, $G_1 \subsetneqq G_2$ なる $G_2 \in \mathscr{L}$ が存在する. これを繰り返すと, $G_1 \subsetneqq G_2 \subsetneqq \cdots \subsetneqq G_n \subsetneqq \cdots$ なる $\mathscr{M}$ の元の無限列が作れ, これは仮定 (b) に矛盾する. (証明終)

Λ-群がネター的となることを見るには, 次の命題を使うと便利である.

命題 8.2 (1) ネター的 Λ-群 G の Λ-部分群 G', および G の Λ-正規部分群による剰余群 G'' は共にネター的である.

(2) Λ-群 G の Λ-正規部分群 G' がネター的で, かつ剰余群 $G'' = G/G'$ もネター的なら, G もネター的である.

(3) 有限個のネター的 Λ-群の直積はネター的である.

[証明] (1) G がネター的なら G' もネター的なことは, 命題 8.1 の (a), (b), (c) のどの条件を使っても明らかである. G がネター的なら, G'' もネター的なことは, 準同型定理と (a), (b), (c) のうちのどれかの条件を使えばわかる.

(2) G の Λ-部分群の無限列 $G_1 \subset G_2 \subset \cdots \subset G_n \subset \cdots$ を考える. これを G' に制限して $G_1 \cap G' \subset G_2 \cap G' \subset \cdots \subset G_n \cap G' \subset \cdots$ を作ると, G' はネター的だから,

ある N' があり $G_{N'} \cap G' = G_{N'+1} \cap G' = \cdots$ となる．また剰余群の方でも，$G_1G'/G' \subset G_2G'/G' \subset \cdots \subset G_nG'/G' \subset \cdots$ において，ある N'' があり，$G_{N''}G'/G' = G_{N''+1}G'/G' = \cdots$ となる．そこで $N = \max(N', N'')$ とおくと，$G_N \cap G' = G_{N+1} \cap G' = \cdots$，および $G_N/G_N \cap G' = G_{N+1}/G_{N+1} \cap G' = \cdots$ が同型定理より成り立つ．よって準同型定理より，$G_N = G_{N+1} = \cdots$ となる．

$G = G' \times G''$ なら，$G' \lhd G$，$G/G' \simeq G''$ であるから，(3) は (2) より明らかである．（証明終）

ネター条件と大小関係を逆にすると次の様になる．

命 題 8. 3 作用域 Λ をもつ群 G について，以下は同値である．

(a) **(極小条件)** G の Λ–部分群の作る空でない集合は，包含関係に関して極小元をもつ．

(b) **(降鎖律)** $G_1 \supset G_2 \supset \cdots \supset G_n \supset \cdots$ を G の Λ–部分群の無限列とすれば，ある番号 N より $G_N = G_{N+1} = \cdots$ となる．

この命題の条件 (a), (b) を満たすとき，Λ–群 G は **アルティン的** であるという．

証明は命題 8.1 と同様にできるので省略する．

またネター条件の場合と同様に，次の命題が成り立つことも証明できる．

命 題 8. 4 (1) アルティン的 Λ–群 G の Λ–部分群 G'，および G の Λ–正規部分群による剰余群 G'' は共にアルティン的である．

(2) Λ–群 G の Λ–正規部分群 G' がアルティン的で，かつ剰余群 $G'' = G/G'$ もアルティン的なら，G もアルティン的である．

(3) 有限個のアルティン的 Λ–群の直積はアルティン的である．

例 8. 5 $\Lambda = \emptyset$，$G = \boldsymbol{Z}$ とする．G の部分群は $m\boldsymbol{Z}$ $(m \in \boldsymbol{Z})$ の形だから，G はネター的である．しかし

$$\boldsymbol{Z} \supsetneqq 2\boldsymbol{Z} \supsetneqq 2^2\boldsymbol{Z} \supsetneqq \cdots \supsetneqq 2^n\boldsymbol{Z} \supsetneqq \cdots$$

であるから，G はアルティン的ではない．

例 8. 6 $\Lambda = \boldsymbol{R}$, G を有限次元 $\boldsymbol{R}$–ベクトル空間とする．このとき G はネター的かつアルティン的となる．

例 8. 7 任意の Λ に対し，有限 Λ–群はネター的かつアルティン的となる．

8. 2 組成列 作用域 Λ をもつ群 G における Λ–部分群の列

$$C: \quad G = G_0 \supset G_1 \supset \cdots \supset G_l = \{1\}$$

で，$G_{i-1} \triangleright G_i$ $(i = 1, 2, \cdots, l)$ となるものを Λ–**正規列** とよび，l をその **長さ** という．このとき l 個の群 $\Gamma_i(C) = G_{i-1}/G_i$ ができる．

$$C': \quad G = G_0' \supset G_1' \supset \cdots \supset G_m' = \{1\}$$

をもう1つの Λ–正規列とする．このとき，$l = m$ でかつ $\{\Gamma_i(C)\}$ と $\{\Gamma_i(C')\}$ が順序の差を除いて一致するなら，C と C' は **同値** であるという．また C' が C の途中にいくつかの項をはさむことによって得られるなら，C' は C の **細分** であるという．とくに，どの G_i とも一致しない G_j' が存在するなら，C' は C の **真の細分** であるという．

定 理 8. 8 （シュライアーの細分定理） C, D を Λ–群 G の Λ–正規列とするとき，C の細分 C' と D の細分 D' で，C' と D' が同値となるものが存在する．

この定理の証明のため，次の補題を証明する．

補 題 8. 9 （ツァッセンハウス） H, K を Λ–群 G の Λ–部分群，H', K' をそれぞれ H, K の Λ–正規部分群とする．このとき $H'(H \cap K') \triangleleft H'(H \cap K)$, $K'(H' \cap K) \triangleleft K'(H \cap K)$ であり，次の Λ–同型が成り立つ：

$$H'(H \cap K)/H'(H \cap K') \simeq K'(H \cap K)/K'(H' \cap K)$$

［証 明］ $H' \triangleleft H$ だから，$H \cap K \subset H'(H \cap K) \subset H \subset N_G(H')$ となる．よって $H'(H \cap K)$, $H'(H \cap K')$ は群となり，$H' \triangleleft H'(H \cap K)$ となる．これを部分群 K に制限すると，$H' \cap K \triangleleft (H' \cap K)(H \cap K) = H \cap K$ となる．よって同型定理により，Λ–同型

$$f: \quad (H \cap K)/(H' \cap K) \ \rightleftarrows\ H'(H \cap K)/H'$$

が成り立つ．H と K の対称性より，$K'(H \cap K)$, $K'(H' \cap K)$ も群で，$H \cap K' \triangleleft$

$H \cap K$ が成り立つ.

さて上の Λ-同型 f により，$(H' \cap K)(H \cap K')$ には $H'(H \cap K')$ が対応し，これらは Λ-正規部分群を定めている．よって f の両辺を，これら対応する Λ-正規部分群で割ると，系2.4より

$$(H \cap K)/(H' \cap K)(H \cap K') \simeq H'(H \cap K)/H'(H \cap K')$$

なる Λ-同型を得る．H と K の対称性より，Λ-同型

$$(H \cap K)/(H' \cap K)(H \cap K') \simeq K'(H \cap K)/K'(H' \cap K)$$

も得られるから，補題が証明できた.

[定理の証明] $C : G = G_0 \supset G_1 \supset \cdots \supset G_l = \{1\}$，$D : G = H_0 \supset H_1 \supset \cdots \supset H_m = \{1\}$ とし，前補題を考慮において,

$$G_i{}^j = G_i(G_{i-1} \cap H_j), \qquad H_j{}^i = H_j(G_i \cap H_{j-1})$$

とおく．このとき C, D の細分

$$C' : \quad G = G_1{}^0 \supset G_1{}^1 \supset \cdots \supset G_1{}^m = G_1 = G_2{}^0 \supset G_2{}^1 \supset \cdots \supset G_l{}^m = \{1\},$$

$$D' : \quad G = H_1{}^0 \supset H_1{}^1 \supset \cdots \supset H_1{}^l = H_1 = H_2{}^0 \supset H_2{}^1 \supset \cdots \supset H_m{}^l = \{1\}$$

ができる．C' と D' は共に長さが lm で，しかも，ツァッセンハウスの補題より Λ-同型

$$\begin{aligned} G_i{}^{j-1}/G_i{}^j &= G_i(G_{i-1} \cap H_{j-1})/G_i(G_{i-1} \cap H_j) \\ &\simeq H_j(G_{i-1} \cap H_{j-1})/H_j(G_i \cap H_{j-1}) = H_j{}^{i-1}/H_j{}^i \end{aligned}$$

が成り立つ．よって C' と D' は同値である. (証明終)

Λ-群 G の Λ-正規列 $C : G = G_0 \supset G_1 \supset \cdots \supset G_l = \{1\}$ で，$G_{i-1} \neq G_i$ $(i = 1, 2, \cdots, l)$ を満たし，しかも真の細分をもたないものを **Λ-組成列** という．このためには，各 G_{i-1}/G_i が Λ-単純群となることが必要十分である．このとき，これら $\{G_{i-1}/G_i\}$ を **Λ-組成因子** とよぶ．Λ-組成列のことを $\Lambda = \emptyset$ のときは **組成列**，$\Lambda = \mathrm{Inn}(G)$ のときは **主組成列**，$\Lambda = \mathrm{Aut}(G)$ のときは **特性組成列** とよぶ.

例 8.10 S_4 を4次対称群とし，A_4 を4次の交代群とする．S_4 の部分群 V を

$$V = \{1, (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\}$$

で定義し，**クラインの4元群** とよぶ．A_4 は S_4 の偶置換全体から成る正規部分群であり，V も S_4 の単位元と型が 2^2 の置換全体から成る正規部分群である．よって $\Lambda = \mathrm{Inn}(S_4)$

とおくと，

$$C: \quad S_4 \supset A_4 \supset V \supset \{1\}$$

は S_4 の Λ-正規列をなす．$S_4/A_4 \simeq \boldsymbol{Z}/2\boldsymbol{Z}$，$A_4/V \simeq \boldsymbol{Z}/3\boldsymbol{Z}$ だからこれらは単純群である．また $V \simeq (\boldsymbol{Z}/2\boldsymbol{Z}) \times (\boldsymbol{Z}/2\boldsymbol{Z})$ は単純群ではないが，V の上の特徴づけより，Λ-単純となる．よって C は主組成列となる．また C の細分

$$C': \quad S_4 \supset A_4 \supset V \supset \{1, (1\ 2)(3\ 4)\} \supset \{1\}$$

は S_4 の組成列をなす．

定理 8.11 （ジョルダン・ヘルダー） Λ-群 G の任意の 2 つの Λ-組成列は互いに同値である．

［証明］ C, D を G の Λ-組成列とする．このときシュライアーの細分定理により，C, D の細分 C', D' で互いに同値なものが存在する．ところが C, D は組成列だから，C', D' は真の細分ではなく，$\{\Gamma_i(C')\}$，$\{\Gamma_j(D')\}$ は $\{\Gamma_i(C)\}$，$\{\Gamma_j(D)\}$ に単位群をいくつかつけ加えただけである．$\{\Gamma_i(C')\} = \{\Gamma_j(D')\}$ だから，それらより単位群を除いた $\{\Gamma_i(C)\}$ と $\{\Gamma_j(D)\}$ も一致する． （証明終）

一般には，Λ-組成列は存在するとは限らないが，次のことがいえる．

定理 8.12 Λ-部分群に関し極大条件と極小条件を満たす Λ-群は，Λ-組成列をもつ．とくに有限 Λ-群は Λ-組成列をもつ．

［証明］ 有限群の場合は極大・極小条件を満たすのは明らかである．よって定理の最初の部分のみを示せばよい．

G の部分群 H で，Λ-部分群の列

$$C: \quad G = G_0 \supset G_1 \supset \cdots \supset G_l = H, \qquad G_{i-1} \triangleright G_i,\ G_{i-1}/G_i \text{ は } \Lambda\text{-単純}$$

なるものが存在するもの全体を $\mathscr{H}$ で表す．$\mathscr{H} \ni G$ だから $\mathscr{H} \neq \emptyset$ であり，極小条件より $\mathscr{H}$ は包含関係に関して極小な元 H を含む．対応する Λ-部分群の列を上の様に C で表す．もし $H \neq \{1\}$ なら，H の真の Λ-正規部分群の集合 $\mathscr{K}$ は $\emptyset$ ではない．よって極大条件より，$\mathscr{K}$ は極大元をもつ． それを G_{l+1} で表すと，$G_l \triangleright G_{l+1}$ かつ G_l/G_{l+1} は Λ-単純群となる．このとき $C': G = G_0 \supset G_1 \supset \cdots \supset G_l \supset G_{l+1}$ も C と同じ条件を満たし，これは $G_l = H$ の極小性に矛盾する．よって $H = \{1\}$ となり，C は Λ-

組成列となる. (証明終)

(注) $G = SL_2(\boldsymbol{R})/\pm 1$ は単純群だが, $\boldsymbol{R}$ と同型な部分群をもち, 極大条件も極小条件も成り立たない.

8.3 可解群とべき零群 8.3では, $\Lambda = \emptyset$ とし, 作用域は考えないものとする.

G を群, $a, b \in G$ とするとき

$$[a, b] = aba^{-1}b^{-1}$$

とおき, これを a, b の **交換子** とよぶ.

$$ab = ba \iff [a, b] = 1$$

が成り立つから, a, b が可換なことと $[a, b] = 1$ となることは同値である. a, b が G 全体を動くとき, 交換子 $[a, b]$ 全体の生成する G の部分群を $D(G)$ または $[G, G]$ で表し, G の **交換子群** とよぶ. $c[a, b]c^{-1} = [cac^{-1}, cbc^{-1}]$ であるから, $D(G) \lhd G$ であり, また $G/D(G)$ はアーベル群となる. 同様に, H, K を G の部分群とするとき, $[a, b]$ $(a \in H,\ b \in K)$ で生成される G の部分群を $[H, K]$ で表す.

命題 8.13 H を群 G の部分群とする. このとき $H \lhd G$ かつ G/H がアーベル群となるための必要十分条件は, $H \supset D(G)$ なることである.

[証明] $H \lhd G$ で G/H がアーベル群であるとする. このとき, $\forall a, b \in G$ に対し $[a, b]H = H$ となるから, $[a, b] \in H$ となる. 逆に $H \supset D(G)$ なら $G/D(G)$ がアーベル群となるから, その部分群 $H/D(G)$ は正規部分群となる. したがって, 準同型定理より $H \lhd G$ となり, $G/H \simeq (G/D(G))/(H/D(G))$ はアーベル群となる. (証明終)

群 G の正規列 C: $G = G_0 \supset G_1 \supset \cdots \supset G_l = \{1\}$ で, G_{i-1}/G_i $(i = 1, 2, \cdots, l)$ がアーベル群となるものを **アーベル的正規列** とよび, アーベル的正規列をもつ群 G を **可解群** とよぶ.

定理 8.14 G が可解群となるためには, ある l に対し, $D^l(G) = \{1\}$ となることが必要かつ十分である. ここで $D^l(G)$ は $D^i(G) = D(D^{i-1}(G))$ と

帰納的に定義する.

[証明] このような l があれば, $G_i = D^i(G)$ とおくと, アーベル的正規列が得られる. 逆に, C: $G = G_0 \supset G_1 \supset \cdots \supset G_l = \{1\}$ がアーベル的正規列であったとする. このとき G_{i-1}/G_i はアーベル群だから, 命題 8.13 より $G_i \supset D(G_{i-1})$ となる. よって帰納的に $G_l \supset D^l(G)$ となるから, $D^l(G) = \{1\}$ となる. (証明終)

また可解群を次のようにも特徴づけられる.

定理 8.15 有限群が可解群となるためには, その組成因子がすべて素数位数の群となることが必要かつ十分である (例 8.7, 定理 8.12 参照).

[証明] アーベル的正規列を細分して組成列を作れば, 組成因子は単純アーベル群となる. ところが, アーベル群が単純群となるのは, 定理 6.1 と例 2.6 より, 素数位数の巡回群の場合に限る. 素数位数の群はアーベル群だから, 逆は明らかである. (証明終)

可解性の判定には, 次の命題が便利である.

命題 8.16 (1) 可解群の部分群, 剰余群は, ともに可解群である.

(2) $N \triangleleft G$ で, N および G/N が可解群なら, G も可解群である.

(3) 有限個の可解群の直積は可解群である.

[証明] アーベル群の部分群および剰余群はアーベル群である. よって, アーベル的正規列を部分群に制限しても, 自然な準同型で剰余群に移しても, またアーベル的正規列を得る. よって (1) が示せた.

π: $G \longrightarrow G/N$ を自然な準同型とし, $N = N_0 \supset N_1 \supset \cdots \supset N_n = \{1\}$ と $G/N = H_0 \supset H_1 \supset \cdots \supset H_l = \{1\}$ をアーベル的正規列とする. このとき $G_i = \pi^{-1}(H_i)$ とおくと,

$$G = G_0 \supset G_1 \supset \cdots \supset G_l = N = N_0 \supset N_1 \supset \cdots \supset N_n = \{1\}$$

は G のアーベル的正規列となる.

(3) は (2) より明らかである. (証明終)

例 8.17 S_n を n 次対称群とする. 例 8.10 より, A_4 を 4 次の交代群とし, V をクラインの 4 元群とすると, $S_4 \supset A_4 \supset V \supset \{1\}$ はアーベル的正規列となる. よって S_4 は可解群である. S_3, S_2 は S_4 の部分群と同型であるから, S_n ($n \leqq 4$) は可解群である.

このことは第V章で，4次以下の代数方程式が根の公式をもつことを示すのに使われる.

これに対し，次の定理と定理8.15より，対称群 S_n は $n\geqq 5$ のときは可解群ではないことがわかる.

定理 8.18 $n\geqq 5$ なら交代群 A_n は単純群である.

証明のため，まず次の補題を示す.

補題 8.19 $n\geqq 3$ のとき，交代群 A_n は長さ3の巡回置換全体で生成される.

[証明] 長さ3の巡回置換は偶置換であり，A_n に含まれる. また A_n の元は互換の積として表したとき偶数個の互換の積となるから，A_n は2つの互換の積 $\sigma=(i\ j)(k\ l)$ の形に書ける置換の全体で生成されている.

ここで，$\{i,j\}=\{k,l\}$ なら $\sigma=1$ となる. また $\{i,j\}$ と $\{k,l\}$ が1つのみ共通元をもつとすれば，例えばそれを $j=k$ とすると，$\sigma=(i\ j)(j\ l)=(i\ j\ l)$ と長さ3の巡回置換となる. また $\{i,j\}$ と $\{k,l\}$ が共通元をもたないなら，

$$\sigma=(i\ j)(k\ l)=(i\ j)(j\ k)(j\ k)(k\ l)=(i\ j\ k)(j\ k\ l)$$

と変形することにより，長さ3の巡回置換2つの積に書ける. よって交代群 A_n は，長さ3の巡回置換全体により生成されている. (証明終)

[定理の証明] $n\geqq 5$ とし，N を A_n の $\{1\}$ 以外の正規部分群とし，$N=A_n$ となることを示す. このためには，補題より，N がすべての長さ3の巡回置換を含むことをいえばよい.

N が長さ3の巡回置換，例えば $(1\ 2\ 3)$，を含むとする. i,j,k を $1\leqq i,j,k\leqq n$ なる相異なる数とし，

$$\rho=\begin{pmatrix}1 & 2 & 3 & \cdots\\ i & j & k & \cdots\end{pmatrix}$$

の形の S_n の元を1つとる. ρ が偶置換なら $\tau=\rho$，ρ が奇置換なら $\tau=\rho(4\ 5)$ とおく. このとき，$\tau\in A_n$ で，$\tau(1\ 2\ 3)\tau^{-1}=\rho(1\ 2\ 3)\rho^{-1}=(i\ j\ k)$ となる. よって $(i\ j\ k)\in N$ となり，$(i\ j\ k)$ は任意だから，$N=A_n$ となる. したがって，N の1と異なる元のうち，実際に動かす文字の個数が最小なものを σ とし，σ が長さ3の巡回置換となることを示せばよい. そこで，σ が少なくとも4個の元を動かすとし，矛盾を導く.

σを互に共通する文字を含まない巡回置換の積に分解すると，互換ばかりの積となるか，長さが3以上の巡回置換を含む積となるかのいずれかである．そこで，おのおのの場合，σが次の形であるとする：

（1） $\sigma=(1\ 2)(3\ 4)\cdots,$

（2） $\sigma=(1\ 2\ 3\ \cdots)\cdots.$

（2）の場合は，σがちょうど4個の元しか動かさないとすると，σの形よりσは長さ4の巡回置換となり，これは奇置換であるから矛盾である．よって，σは少なくとも5個の文字，例えば 1,2,3,4,5 を動かすとしてよい．(1),(2) のいずれの場合も，$\chi=(3\ 4\ 5)$ で変換すると，

（1′） $\sigma_1=\chi\sigma\chi^{-1}=(1\ 2)(4\ 5)\cdots,$

（2′） $\sigma_1=\chi\sigma\chi^{-1}=(1\ 2\ 4\ \cdots)\cdots$

となり，$\sigma\neq\sigma_1$ である．さらに $k>5$ ならkはχで動かないから，$k>5$ がσで動かないなら$\sigma^{-1}\sigma_1$ でも動かない．$\sigma^*=\sigma^{-1}\sigma_1$ とおくと，いずれの場合もσ^*は1を動かさない．（1）の場合は，σ^*は2も動かさないから，(σは5を動かさずσ^*が5を動かす可能性を含めても,) σ^*で動かない文字の数はσで動かない文字の数より少ない．（2）の場合も，σは 1,2,3,4,5 をすべて動かし，σ^* は1を動かさないから，σ^*で不変な文字の数はσで不変な文字の数より少ない．これはσの最小性に矛盾する． （証明終）

群Gの正規列 $C:\ G=G_0\supset G_1\supset\cdots\supset G_l=\{1\}$ で

$$G\triangleright G_i,\qquad G_{i-1}/G_i\subset Z(G/G_i)$$

となるものを **中心列** といい，中心列の存在する群Gを **べき零群** とよぶ．中心は可換だから，べき零群は可解群である．また群Gの真部分群Mで，$G\supsetneqq H\supsetneqq M$ なるGの部分群Hが存在しないものを **極大部分群** という．

問題 8.20 次のことを示せ．

（1） べき零群の部分群および剰余群は，またべき零群となる．

（2） 有限個のべき零群の直積は，またべき零群となる．

命題 8.21 べき零群Gの真部分群をKとすると，$K\subsetneqq N_G(K)$ が成り立つ．したがって，べき零群の極大部分群は正規部分群となる．

[証 明] 前のように中心列 C をとると，$G \supsetneqq K$ であるから，ある i に対し $K \not\supset G_{i-1}$，$K \supset G_i$ が成り立つ．ところが $G_{i-1}/G_i \subset Z(G/G_i)$ であるから，任意の $a \in G_{i-1}$ と $b \in K$ について，$[a,b] = aba^{-1}b^{-1} \in G_i \subset K$ となる．よって $aba^{-1} \in K$ となる．これは $a \in N_G(K)$ を意味するから，$G_{i-1} \subset N_G(K)$ が成り立つ．ところが $G_{i-1} \not\subset K$ だから，$K \subsetneqq N_G(K)$ が成り立つ． (証明終)

この命題を使うと，有限べき零群が次のようにして特徴づけられる．

定 理 8. 22 G を有限群とすると，次は同値である．

（1） G はべき零群である．

（2） G の任意の極大部分群は正規部分群である．

（3） G のシロー部分群はすべて正規部分群である．

（4） G はいくつかの p–群（p は動く）の直積である．

証明の前に次の補題を示す．

補 題 8. 23 G を有限群，N を G の正規部分群，P を G のシロー p–部分群とする．このとき，$N \supset P$ なら $G = N \cdot N_G(P)$ となる．

[証 明] a を G の任意の元とすると，P と aPa^{-1} は共に N のシロー p–部分群となる．よってシローの定理より，$b \in N$ があり $bPb^{-1} = aPa^{-1}$ と書ける．このとき $b^{-1}a \in N_G(P)$ となるから，$a = b(b^{-1}a) \in N \cdot N_G(P)$ となる． (証明終)

[定理の証明] （1）$\Longrightarrow$（2）は前命題より明らかである．

（2）$\Longrightarrow$（3）． P を G のシロー p–部分群とし，$N_G(P) \subsetneqq G$ とする．G は有限群だから，$N_G(P)$ を含む G の極大部分群 M が存在する．このとき仮定（2）より $M \lhd G$ となるが，さらに補題を使うと $G = M \cdot N_G(P) = M$ が成り立つ．これは $M \neq G$ という仮定に矛盾する．

（3）$\Longrightarrow$（4）． $|G| = p_1^{e_1} p_2^{e_2} \cdots p_t^{e_t}$ と素因数分解し，各素数 p_i について，シロー p_i–部分群 P_i をとる．仮定（3）より $P_i \lhd G$ であるが，$|P_i| = p_i^{e_i}$ $(i = 1, 2, \cdots, t)$ は互いに素でもある．よって，j に関する帰納法で，$|P_1 \cdot P_2 \cdot \cdots \cdot P_j| = p_1^{e_1} p_2^{e_2} \cdots p_j^{e_j}$，$(P_1 \cdot P_2 \cdot \cdots \cdot P_{j-1}) \cap P_j = \{1\}$ $(j = 2, 3, \cdots, t)$ がわかる．よって定理 5.2（と問題 5.3）より，$G = P_1 \times P_2 \times \cdots \times P_t$ となる．

（4）$\Longrightarrow$（1）．有限個のべき零群の直積はべき零群となる（問題 8.20 参照）から，p-群がべき零群となることを示せばよい．G を p-群，$\neq \{1\}$ とし，G の位数に関する帰納法で示す．§3の類等式において，G が p-群だから，$|G|$ と $|C_i| \neq 1$ はすべて p で割り切れる．よって，G の中心の位数 $|Z(G)|$ も p で割り切れるから，$Z(G) \neq \{1\}$ である．よって，$G/Z(G)$ は位数が $|G|$ より小さい p-群だから，帰納法の仮定によりべき零群となる．π：$G \longrightarrow G/Z(G) = G'$ を自然な準同型とし，C'：$G' = G_0' \supset G_1' \supset \cdots \supset G_l' = \{1\}$ を中心列とする．このとき $G_i = \pi^{-1}(G_i')$ とおくと，C：$G = G_0 \supset G_1 \supset \cdots \supset G_l = Z(G) \supset \{1\}$ は，準同型定理より $G \triangleright G_i$，$G_{i-1}/G_i \simeq G_{i-1}'/G_i' \subset Z(G'/G_i') \simeq Z(G/G_i)$ となり，G の中心列となる．よって G はべき零群となる．　　　（証明終）

例 8.24　p, q を素数，$p > q$ とし，G を位数 pq の有限群とする．例 4.2 より，G のシロー p-部分群 P は正規である．G のシロー q-部分群を Q とすると，Q は正規部分群となるとは限らないが，$G = P \cdot Q$，$P \cap Q = \{1\}$ となっている．よって

$$Q \triangleleft G \iff G = P \times Q \iff G \text{ はアーベル群}$$

となる．いい直すと，アーベル的でない位数 pq の有限群は，べき零群でない．例えば，対称群 S_3 はべき零群ではない．

§9. 生成元と基本関係*

X を集合とする．このとき，各 $x \in X$ に対して新しい文字 x^{-1} を考え，

$$X^{-1} = \{x^{-1} \mid x \in X\}, \qquad \tilde{X} = X \amalg X^{-1}$$

とおく．

$\tilde{X}$ の元を有限個並べたものを $\boldsymbol{x} = (x_1, x_2, \cdots, x_m)$ $(x_i \in X$ または $x_i \in X^{-1}, m \geqq 0)$ のように表し，このような元 $\boldsymbol{x}$ の全体を $W(X)$ とおく．そこで $W(X)$ の積を，

$$(x_1, x_2, \cdots, x_m) \cdot (y_1, y_2, \cdots, y_n) = (x_1, x_2, \cdots, x_m, y_1, y_2, \cdots, y_n)$$

で定義すると，この積は結合法則を満たす．さらに，$\tilde{X}$ の元0個を並べたもの（　）を1で表すと，1は $W(X)$ の単位元となる．

$\boldsymbol{x}=(x_1,x_2,\cdots,x_m)\in W(X)$ とするとき，ある $1\leqq \boldsymbol{i}<\boldsymbol{m}$ に対し，

$x_i\in X$, $x_{i+1}={x_i}^{-1}\in X^{-1}$, または　$x_{i+1}\in X$, $x_i={x_{i+1}}^{-1}\in X^{-1}$

となるとき，$(x_1,x_2,\cdots,x_{i-1},x_{i+2},\cdots,x_m)$ は $\boldsymbol{x}$ より x_i と x_{i+1} を **簡約** して得られるという．

一般に，$\boldsymbol{x},\boldsymbol{y}\in W(X)$ は，適当な $W(X)$ の元の列 $\boldsymbol{u}_0=\boldsymbol{x},\boldsymbol{u}_1,\cdots,\boldsymbol{u}_n=\boldsymbol{y}$ があり，各 $0\leqq \boldsymbol{i}<\boldsymbol{n}$ に対し，（a） $\boldsymbol{u}_{i+1}$ が $\boldsymbol{u}_i$ の 2 元を簡約して得られるか，（b） $\boldsymbol{u}_i$ が $\boldsymbol{u}_{i+1}$ の 2 元を簡約して得られるとき，$\boldsymbol{x}$ と $\boldsymbol{y}$ は **同値** であるといい，$\boldsymbol{x}\sim\boldsymbol{y}$ と表す．

この関係 $\boldsymbol{x}\sim\boldsymbol{y}$ は同値関係をなし，それによる $W(X)$ の商集合を $F(X)$ で表し，**X で生成される自由群** とよぶ．

実際，同値関係の定義より，

$$\boldsymbol{x}_1\sim\boldsymbol{x}_2,\ \ \boldsymbol{y}_1\sim\boldsymbol{y}_2 \implies \boldsymbol{x}_1\cdot\boldsymbol{y}_1\sim\boldsymbol{x}_2\cdot\boldsymbol{y}_2$$

だから，$W(X)$ の積は $F(X)$ の積を定め，この積に関し $F(X)$ は，1 の類を単位元，

$$(x_1,x_2,\cdots,x_m)^{-1}\sim({x_m}^{-1},{x_{m-1}}^{-1},\cdots,{x_1}^{-1})$$

を逆元とする群となる．ここで $x_i={y_i}^{-1}\in X^{-1}$ のときは，${x_i}^{-1}=y_i$ とする．

G を群とし，G は部分集合 S で群として生成されるものとする．このとき，

$$W(S)\ni(s_1,s_2,\cdots,s_n) \longmapsto s_1s_2\cdots s_n\in G$$

は，$(s_1,s_2,\cdots,s_n)$ の同値類のとり方によらずに定まり，

$$\boldsymbol{i}:\ \ F(S)\longrightarrow G$$

なる群の準同型を与える．しかも $\boldsymbol{i}(S)\supset S$ だから，$\mathrm{Im}(\boldsymbol{i})=G$ となる．よって $\boldsymbol{i}$: $F(S)\longrightarrow G$ は自由群 $F(S)$ から群 G への全射な準同型となる．とくに，$G\simeq F(S)/\mathrm{Ker}(\boldsymbol{i})$ となる．

$\boldsymbol{i}$: $F(S)\longrightarrow G$ を上のようなものとするとき，S を G の **生成元** とよび，$\mathrm{Ker}(\boldsymbol{i})\subset F(S)$ の元を $=1$ とおいたものを，S の元の間にある **関係式** とよぶ．特に $R\subset F(S)$ とするとき，R の類を含む最小の $F(S)$ の正規部分群が $\mathrm{Ker}(\boldsymbol{i})$ となるなら，R の元を $=1$ とおいたものの集合を，G の生成元 S に

関する **基本関係** とよぶ．この場合，

$$G = \langle S \mid r = 1 \ (\forall r \in R) \rangle$$

などとして，G を表すことがある．

例 9．1 対称群 S_n は，$S = \{\sigma_i = (i, i+1) \mid 1 \leqq i \leqq n-1\}$ を生成元とし，

$$\sigma_i{}^2 = 1 \qquad (1 \leqq i \leqq n-1), \qquad (\sigma_i \sigma_{i+1})^3 = 1 \qquad (1 \leqq i \leqq n-2),$$

$$(\sigma_i \sigma_j)^2 = 1 \qquad (1 \leqq i, j \leqq n, \ |i-j| \geqq 2)$$

を基本関係としてもつ．

例 9．2 $X = \{\sigma, \tau\}$ で生成される自由群 F を，

$$\sigma^n, \quad \tau^2, \quad \tau^{-1}\sigma\tau\sigma \qquad (n \in \boldsymbol{N})$$

を含む最小の正規部分群 R で割った剰余群を，

$$D_n = \langle \sigma, \tau \mid \sigma^n = 1, \ \tau^2 = 1, \ \tau^{-1}\sigma\tau = \sigma^{-1} \rangle$$

と表し，**2 面体群** とよぶ．D_n は $\langle \sigma \mid \sigma^n = 1 \rangle$ を正規部分群としてもち，$D_n / \langle \sigma \mid \sigma^n = 1 \rangle \simeq \langle \tau \mid \tau^2 = 1 \rangle$ を剰余群としてもつから，位数 $2n$ の有限群となる．

問　　題

1． G を群，H を G の指数有限の部分群とする．このとき H は指数有限の G の正規部分群を含むことを示せ．

2． G を有限群，Z を G の中心とする．このとき，G/Z が巡回群なら G はアーベル群となることを示せ．

3． p を素数とするとき次を示せ．

（1） 位数 p^2 の群はアーベル群である．

（2） G を位数 p^3 の非アーベル的な群とし，Z を G の中心とする．このとき $G/Z \simeq \boldsymbol{Z}/p\boldsymbol{Z} \times \boldsymbol{Z}/p\boldsymbol{Z}$ となる．

4． G を有限群で，ちょうど 2 個の自明でない部分群をもつものとする．このとき G は，（1）位数 p^3 の巡回群（p は素数），または（2）位数が pq の巡回群（p, q は相異なる素数）のどちらかと同型となることを示せ．

5.　位数 2275 の有限群はアーベル群であることを示せ.

6.　k を有限個の元から成る体とし，$\#(k) = q$ とおく．このとき，k 上の一般線型群 $GL(n, k)$ の位数は，$(q^n - 1)(q^n - q)\cdots(q^n - q^{n-1})$ となることを示せ.

7.　$n \geqq 3$ のとき，n 次対称群 S_n の中心は単位元に限ることを示せ.

8.　群 G が指数 n $(2 \leqq n \leqq 4)$ の部分群 $\neq \{1\}$ をもてば，単純群でないことを示せ.

9.　G を有限アーベル群とし，χ を G から 0 でない複素数全体の作る乗法群 $\boldsymbol{C}^*$ への準同型写像とする．このとき

$$\sum_{g \in G} \chi(g) = \begin{cases} |G| & \chi(g) \equiv 1 \text{ のとき} \\ 0 & \text{その他} \end{cases}$$

となることを示せ.

10.　G をべき零群，Z を G の中心とする．G の正規部分群 $N \neq \{1\}$ は $N \cap Z \neq \{1\}$ を満たすことを示せ.

11.　$G = SL_2(\boldsymbol{R})$ とする．このとき

$$i:\quad G \ni \begin{pmatrix} a & b \\ c & d \end{pmatrix} \longmapsto \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}^{-1} \in G$$

は，G の自己同型だが，内部自己同型ではないことを示せ.

12.　$\chi:\ S_4 \longrightarrow \boldsymbol{T} = \{z \in \boldsymbol{C} \mid |z| = 1\}$ なる準同型写像をすべて求めよ.

13.　p を素数，$G = (\boldsymbol{Z}/p^3\boldsymbol{Z}) \times (\boldsymbol{Z}/p^2\boldsymbol{Z})^2$ とおく．このとき，G の自己同型群 $\mathrm{Aut}(G)$ の位数を求めよ.

14.　有理数の加法のなす群 $\boldsymbol{Q}$ は直既約だが，剰余群 $\boldsymbol{Q}/\boldsymbol{Z}$ は直既約ではないことを示せ.

15.　有限群 G は，位数 2 の元がちょうど半分あり，残り半分が部分群 H をなすものとする．このとき，

（1）H は奇数位数のアーベル群であることを示せ.

（2）このような群 G の例を複数個あげよ.

III　環

集合 R 上に和 $+$ と積・が定義されており，$+$ に関して 0 を単位元とするアーベル群，・に関し $1 \neq 0$ を単位元とする半群となり，かつ $+$ と・とが分配法則によって関係づけられているものを環という（第 I 章，§6 参照）．この章では，主に可換環の性質を調べる．環の性質のうち，環上の加群の性質と考えた方が適切なもの（単因子の理論，半単純環の理論など）は，加群の章で扱う．

§1. イデアルと準同型定理

1.1 イデアル　R を加法 $+$ と乗法・の定義された環とし，R の零元（加法の単位元）を 0 で表し，R の乗法に関する単位元を 1 で表す．R の部分集合 S は，R の演算 $+$ と・に関し，

$$a, b \in S \implies a \pm b,\ a \cdot b \in S$$

を満たし，かつ $1 \in S$ となるなら，それ自身環となる．このような部分集合 S を **部分環** とよぶ．例えば，R の **中心**

$$C(R) = \{a \in R \mid ax = xa \ \ (\forall x \in R)\}$$

は，可換な部分環をなす．

R の部分集合 $\mathfrak{a}$ は，

(I 1)　加法について部分群をなす，

(I 2)　$r \in R,\ a \in \mathfrak{a} \implies r \cdot a \in \mathfrak{a}$

を満たすとき **左イデアル** であるという．同様に，R の部分集合 $\mathfrak{a}$ が，(I 1) と

(I 3)　$r \in R,\ a \in \mathfrak{a} \implies a \cdot r \in \mathfrak{a}$

を満たすとき **右イデアル** であるといい，(I 1), (I 2), (I 3) を満たすとき **両側**

イデアル であるという．R が可換環のときは，これらの区別は不要だから，単に **イデアル** という．

一般に，R および $\{0\}$ は R の両側イデアルをなすが，これらを **自明なイデアル** とよび，自明なイデアル以外両側イデアルをもたない環を **単純環** とよぶ．環 R の左(右)イデアル $\mathfrak{a}$ が $R=\mathfrak{a}$ となるには，$\mathfrak{a}\ni 1$ となることが必要かつ十分である．

$\mathfrak{a},\mathfrak{b}$ を環 R の左(右)イデアルとすると，$\mathfrak{a}$ と $\mathfrak{b}$ の **交わり** $\mathfrak{a}\cap\mathfrak{b}$ は，$\mathfrak{a}$ と $\mathfrak{b}$ に含まれる左(右)イデアルのうち最大のものとなる．また $\mathfrak{a}$ と $\mathfrak{b}$ の **和**

$$\mathfrak{a}+\mathfrak{b}=\{a+b \mid a\in\mathfrak{a},\ b\in\mathfrak{b}\}$$

は，$\mathfrak{a}$ と $\mathfrak{b}$ を含む左(右)イデアルのうち最小のものとなる．さらに，$\mathfrak{a},\mathfrak{b}$ が共に両側イデアルなら，$\mathfrak{a}$ と $\mathfrak{b}$ の **積**

$$\mathfrak{a}\cdot\mathfrak{b}=\{\sum_i a_ib_i\ (\text{有限和}) \mid a_i\in\mathfrak{a},\ b_i\in\mathfrak{b}\}$$

も $\mathfrak{a}$ と $\mathfrak{b}$ に含まれる両側イデアルとなる．よって，$\mathfrak{a}\cdot\mathfrak{b}\subset\mathfrak{a}\cap\mathfrak{b}$ となるが，一般には等号は成り立たない．

$a\in R$ のとき，$Ra=\{ra \mid r\in R\}$ は R の左イデアルとなる．これを a で生成される **単項左イデアル** とよぶ．**単項右イデアル** aR も同様に定義される．

一般に，X を R の部分集合とするとき，

$$\sum a_ix_i \qquad (a_i\in R,\ x_i\in X)$$

なる有限和の全体を RX で表す．RX は，X を含む R の左イデアルとなる．これを X で **生成** される左イデアルとよぶ．X で生成される右イデアル XR も同様に定義される．R が可換環なら，$RX=XR$ となる．このとき，X が有限個の元 $a_1,a_2,\cdots,a_n$ から成るなら，RX を $(a_1,a_2,\cdots,a_n)$ と表す．

命題 1.1　環 R が斜体となるための必要十分条件は，R が自明でない左(右)イデアルをもたないことである．

［証明］（必要性）　R を斜体とし，$\mathfrak{a}$ を R の $\{0\}$ 以外の左イデアルとする．$\mathfrak{a}\ni a\neq 0$ とすると，a は逆元 a^{-1} をもつ．よって，$\mathfrak{a}\ni a^{-1}a=1$ となり，$\mathfrak{a}=R$ となる．

（十分性）　R の左イデアルは，R と $\{0\}$ のみであるとする．a を R の 0 でない元

とすると，単項左イデアル Ra は，$1\cdot a = a$ を含むから $\{0\}$ ではない．よって $Ra = R$ となるから，$ba = 1$ となる元 $b \in R$ が存在する．$b \neq 0$ であるから，同様にして，$cb = 1$ となる元 $c \in R$ も存在する．このとき

$$c = c1 = c(ba) = (cb)a = 1a = a$$

であるから，

$$ab = 1, \qquad ba = 1$$

となる．よって b は a の逆元である．（証明終）

例 1. 2 D を環とし，$R = M_n(D)$ を D に成分をもつ $n \times n$ 行列全体のなす環とする．e_{ij} で (i,j) 成分のみが 1 で他は 0 の R の行列を表す．このとき，

$$Re_{ij} = \left\{ \begin{pmatrix} & * & \\ 0 & \vdots & 0 \\ & * & \end{pmatrix} \right\}, \qquad e_{ij}R = \left\{ \begin{pmatrix} & 0 & \\ * & \cdots\cdots & * \\ & 0 & \end{pmatrix} \right\}$$

と，単項左イデアル Re_{ij} は第 j 列以外 0 の R の行列全体と一致し，単項右イデアル $e_{ij}R$ は第 i 行以外 0 の R の行列全体と一致する．

D を斜体とし，$\mathfrak{a}$ を R の $\{0\}$ でない両側イデアルとし，$A = (a_{ij})$ を $\mathfrak{a}$ の 0 でない元とする．

$A \neq 0$ だから，ある A の成分 a_{ij} は 0 でない．D は斜体だから，$a_{ij} \neq 0$ の逆元を $a_{ij}{}^{-1}$ とすると $\mathfrak{a}$ は $(a_{ij}{}^{-1}e_{ii})Ae_{jj} = e_{ij}$ を含む．$e_{ki}e_{ij}e_{jl} = e_{kl}$ であるから，$\mathfrak{a}$ は単位行列 $E_n = e_{11} + e_{22} + \cdots + e_{nn}$ を含む．よって $\mathfrak{a} = R$ となる．これより斜体上の行列環が単純環となることがわかる．

問題 1. 3 $\mathfrak{a}, \mathfrak{b}$ を可換環 R のイデアルとし，$\mathfrak{a} + \mathfrak{b} = R$ が成り立つとする．このとき，$\mathfrak{a}\mathfrak{b} = \mathfrak{a} \cap \mathfrak{b}$ が成り立つことを示せ．

1. 2 剰余環と準同型定理 R を環とし，$\mathfrak{a}$ を R の両側イデアルで，$\mathfrak{a} \neq R$ とする．$\mathfrak{a}$ は和に関し R の正規部分群をなすから，剰余群 $R/\mathfrak{a}$ を作る．

$$R/\mathfrak{a} = \{a + \mathfrak{a} \mid a \in R\}$$

であり，$R/\mathfrak{a}$ には和が

$$(a + \mathfrak{a}) + (b + \mathfrak{a}) = (a + b) + \mathfrak{a}$$

で定まっている．$R/\mathfrak{a}$ における積を

$$(a+\mathfrak{a})\cdot(b+\mathfrak{a}) = a\cdot b+\mathfrak{a}$$

で定義する．$a+\mathfrak{a}=a'+\mathfrak{a}$, $b+\mathfrak{a}=b'+\mathfrak{a}$ なら，$a'=a+a''$，$b'=b+b''$ $(a'',b''\in\mathfrak{a})$ と書くと，$\mathfrak{a}$ は両側イデアルだから，

$$a'b'-ab=ab''+a''b+a''b''\in\mathfrak{a}$$

となる．よって上の積の定義は，a,b の選び方によらずに，一意的に定まっている．

$R/\mathfrak{a}$ に和と積をこの様に定義すると，R において結合法則と分配法則が成り立つから，$R/\mathfrak{a}$ でも結合法則と分配法則が成り立ち，$R/\mathfrak{a}$ は $0+\mathfrak{a}$ を零元，$1+\mathfrak{a}$ を単位元とする環をなすことがわかる．この環 $R/\mathfrak{a}$ を，R の両側イデアル $\mathfrak{a}$ による **剰余環** とよぶ．

環 R から環 R' への写像 $f: R\longrightarrow R'$ は，

$$f(a+b)=f(a)+f(b)$$
$$f(a\cdot b)=f(a)\cdot f(b)$$
$$f(1_R)=1_{R'}$$

を満たすとき，（環の）**準同型写像**（または **準同型**）とよぶ．とくに全単射な準同型を **同型写像**（または **同型**）とよび，R と R' は **同型** である，$R\simeq R'$ などと表す．

$f: R\longrightarrow R'$ を環の準同型にするとき，

$$\mathrm{Im}(f)=\{f(a)\mid a\in R\}$$

を f の **像** とよび，

$$\mathrm{Ker}(f)=\{a\in R\mid f(a)=0\}$$

を f の **核** とよぶ．準同型写像の定義より，$\mathrm{Im}(f)$ は R' の部分環であることがすぐわかる．また $r\in R$, $a\in\mathrm{Ker}(f)$ なら，

$$f(ra)=f(r)f(a)=0,\qquad f(ar)=f(a)f(r)=0$$

となるから，$ra, ar\in\mathrm{Ker}(f)$ となる．さらに，$1_{R'}\neq 0_{R'}$ であるから，$\mathrm{Ker}(f)\not\ni 1_R$ である　よって $\mathrm{Ker}(f)$ は，$\mathrm{Ker}(f)\subsetneqq R$ なる R の両側イデ

アルである．

$\mathfrak{a}$ が環 R の両側イデアルで，$\mathfrak{a} \neq R$ だとする．このとき

$$\pi: \quad R \ni a \longmapsto a + \mathfrak{a} \in R/\mathfrak{a}$$

は，環 R より剰余環 $R/\mathfrak{a}$ への全射な準同型写像となる．これを **自然な準同型** とよぶ．このとき，

$$\mathrm{Ker}(\pi) = \mathfrak{a}$$

であるから，環 R の部分集合 $\mathfrak{a}$ が R の両側イデアル（$\neq R$）となるための必要十分条件は，$\mathfrak{a}$ がある環準同型 $f: R \longrightarrow R'$ の核になることである．

$\pi: R \longrightarrow R/\mathfrak{a}$ も自然な準同型とするとき，$\pi(a) = a + \mathfrak{a}$ を $\bar{a}$ や $a \bmod \mathfrak{a}$ と表し，$\pi(a) = \pi(b)$ となることを

$$a \equiv b \pmod{\mathfrak{a}}$$

と表す．

群の場合と同様に，環の場合にも準同型定理が成り立つ：

定理 1.4（準同型定理） R, R' を環とし，$f: R \longrightarrow R'$ を環の準同型とする．このとき，$a + \mathrm{Ker}(f) \longmapsto f(a)$ なる対応により，環として

$$R/\mathrm{Ker}(f) \simeq \mathrm{Im}(f)$$

となる．とくに f が全射なら，$R/\mathrm{Ker}(f) \simeq R'$ となる．

また R の $\mathrm{Ker}(f)$ を含む両側イデアル $\mathfrak{a}$ と，$\mathrm{Im}(f)$ の両側イデアル $\mathfrak{a}'$ とは，

$$\mathfrak{a} = f^{-1}(\mathfrak{a}') \quad \longleftrightarrow \quad \mathfrak{a}' = f(\mathfrak{a})$$

なる対応で 1 対 1 に対応し，環同型 $R/\mathfrak{a} \simeq \mathrm{Im}(f)/\mathfrak{a}'$ が成り立つ．

［証明］ 群の準同型定理より，$a + \mathrm{Ker}(f) \longmapsto f(a)$ なる対応が，加法群としての同型 $R/\mathrm{Ker}(f) \simeq \mathrm{Im}(f)$ をひきおこすことは明らかである．ところが，

$$(a + \mathrm{Ker}(f))\cdot(b + \mathrm{Ker}(f)) = a\cdot b + \mathrm{Ker}(f) \quad \longmapsto \quad f(a\cdot b) = f(a)f(b)$$

であるから，この写像は環としての同型になっている．よって定理の前半が成り立つ．

群についての準同型定理とその系より，$\mathrm{Ker}(f)$ を含む R の部分群 $\mathfrak{a}$ と $\mathrm{Im}(f)$ の部分群 $\mathfrak{a}'$ とが，$\mathfrak{a} = f^{-1}(\mathfrak{a}')$，$\mathfrak{a}' = f(\mathfrak{a})$ なる対応で 1 対 1 に対応する．そこで，$\mathfrak{a}$ が

$\mathrm{Ker}(f)$ を含む R の両側イデアルなら，$\mathfrak{a}' = f(\mathfrak{a})$ は $\mathrm{Im}(f)$ の両側イデアルとなり，逆に $\mathfrak{a}'$ が $\mathrm{Im}(f)$ の両側イデアルなら，$\mathfrak{a} = f^{-1}(\mathfrak{a}')$ が $\mathrm{Ker}(f)$ を含む R の両側イデアルとなることがわかれば，部分群の間の 1 対 1 対応を制限して，両側イデアルの間の 1 対 1 対応が得られる．ところが

$$f(ra) = f(r)f(a), \qquad f(ar) = f(a)f(r)$$

であるから，$a \in f^{-1}(\mathfrak{a}')$ なら $f(a) \in \mathfrak{a}'$ となり，$ra, ar \in f^{-1}(\mathfrak{a}')$ となる．また $f(a) \in f(\mathfrak{a})$ なら，$a \in \mathfrak{a}$ となり，$f(r)f(a) = f(ra) \in f(\mathfrak{a})$，$f(a)f(r) = f(ar) \in f(\mathfrak{a})$ となる．よって $f^{-1}(\mathfrak{a}')$ と $f(\mathfrak{a})$ が両側イデアルとなることがわかった．

さらにこのとき，

$$g: \quad R \ni a \longmapsto f(a) + \mathfrak{a}' \in \mathrm{Im}(f)/\mathfrak{a}'$$

なる写像は環の準同型であり，全射かつ $\mathrm{Ker}(g) = f^{-1}(\mathfrak{a}') = \mathfrak{a}$ となる．よって定理の前半より，$R/\mathfrak{a} \simeq \mathrm{Im}(f)/\mathfrak{a}'$ となる．　（証明終）

例 1. 5　$R = \boldsymbol{Z}$, $m \in \boldsymbol{Z}$, $\mathfrak{a} = m\boldsymbol{Z} = \{ma \mid a \in \boldsymbol{Z}\}$ とおく．$\mathfrak{a}$ は R の m で生成される単項イデアルである．第 I 章，§6，例 6. 2 で環 $\boldsymbol{Z}/m\boldsymbol{Z}$ を定義したが，そこでの記号といまの記号の関係は，

$$a \equiv b \pmod{m} \iff a \equiv b \pmod{\mathfrak{a}}$$

となっている．よって，第 I 章, §6，例 6. 2 の有限環 $\boldsymbol{Z}/m\boldsymbol{Z}$ は，R のイデアル $\mathfrak{a}$ による剰余環 $R/\mathfrak{a}$ とみなせる．

問 題 1. 6　S を環 R の部分環，$\mathfrak{a}$ を R の両側イデアルとする．このとき，$S \cap \mathfrak{a}$ は S の両側イデアルをなし，環同型 $S/S \cap \mathfrak{a} \simeq (S + \mathfrak{a})/\mathfrak{a}$ が成り立つことを示せ．

1. 3　環の直和　$R_1, R_2, \cdots, R_n$ を環とするとき，これらの加法群としての直積を作り，それを $R_1 \oplus R_2 \oplus \cdots \oplus R_n$ で表す．

$$R_1 \oplus R_2 \oplus \cdots \oplus R_n = \{(a_1, a_2, \cdots, a_n) \mid a_1 \in R_1,\ a_2 \in R_2,\ \cdots,\ a_n \in R_n\}$$

であり，これには和が，

$$(a_1, a_2, \cdots, a_n) + (b_1, b_2, \cdots, b_n) = (a_1 + b_1,\ a_2 + b_2,\ \cdots,\ a_n + b_n)$$

で定義されている．$R_1, R_2, \cdots, R_n$ は環であるから，

$$(a_1, a_2, \cdots, a_n) \cdot (b_1, b_2, \cdots, b_n) = (a_1 \cdot b_1,\ a_2 \cdot b_2,\ \cdots,\ a_n \cdot b_n)$$

として積を定義する．これらの演算は，成分ごとの演算により定義されているから，結合法則，分配法則を満たし，$R_1 \oplus R_2 \oplus \cdots \oplus R_n$ は環となる．$R_1 \oplus R_2 \oplus \cdots \oplus R_n$ を，環 $R_1, R_2, \cdots, R_n$ の **直和** とよぶ．

$R = R_1 \oplus R_2 \oplus \cdots \oplus R_n$, $1_R = (1_{R_1}, 1_{R_2}, \cdots, 1_{R_n})$ とおく．環 R_i $(i = 1, 2, \cdots, n)$ を自然なうめ込み $R_i \ni a_i \longmapsto (0, \cdots, 0, a_i, 0, \cdots, 0) \in R$ により R の部分集合と思い，またこのうめ込みで，R_i の元を R の元と思う．このとき，1_{R_i} は R の中心 $C(R)$ に入り，

$$1_R = 1_{R_1} + 1_{R_2} + \cdots + 1_{R_n}, \qquad 1_{R_i} \cdot 1_{R_i} = 1_{R_i},\ 1_{R_i} \cdot 1_{R_j} = 0 \quad (i \neq j)$$

が成り立つ．また $R_i = R \cdot 1_{R_i} = 1_{R_i} \cdot R$ と書けるから，R_i は R の両側イデアルとなる．

一般に環 R の元 e は，$e^2 = e$ を満たすとき **べき等元** とよび，R の中心 $C(R)$ に属するべき等元を，**中心べき等元** という．このとき上の逆が成り立つ：

命題 1.7 $e_1, e_2, \cdots, e_n$ を環 R の中心べき等元とし，$1_R = e_1 + e_2 + \cdots + e_n$，$e_i \cdot e_j = 0$ $(i \neq j)$ が成り立つものとする．このとき，$R_i = R \cdot e_i$ は R の両側イデアルであり，R_i を単位元 e_i をもつ環と思うと，次の環の同型が成り立つ：

$$R \simeq R_1 \oplus R_2 \oplus \cdots \oplus R_n$$

［証明］ $f : R \ni a \longmapsto (ae_1, ae_2, \cdots, ae_n) \in R_1 \oplus R_2 \oplus \cdots \oplus R_n$ とおく．f は加群の準同型であり，$e_i \in C(R)$ より $R_i = R \cdot e_i$ は R の両側イデアルとなる．$1 = e_1 + e_2 + \cdots + e_n$ だから，f は単射である．また $e_i{}^2 = e_i$ より $(ab)e_i = abe_i{}^2 = (ae_i)(be_i)$ となり，f は環準同型である．さらに $e_i e_j = 0$ $(i \neq j)$ だから，任意の $a_1 e_1 \in R_1$, $a_2 e_2 \in R_2$, $\cdots$, $a_n e_n \in R_n$ に対して，$f(a_1 e_1 + a_2 e_2 + \cdots + a_n e_n) = (a_1 e_1, a_2 e_2, \cdots, a_n e_n)$ となる．よって f は全射である．（証明終）

環の直和分解については，次の命題も便利である．

命題 1.8 $\mathfrak{a}_1, \mathfrak{a}_2, \cdots, \mathfrak{a}_n$ を環 R の両側イデアルで，$\mathfrak{a}_i + \mathfrak{a}_j = R$ $(i \neq j)$ が成り立つものとする．このとき，

（1） $\mathfrak{a}_i + \bigcap_{j \neq i} \mathfrak{a}_j = R$ $(i = 1, 2, \cdots, n)$ が成り立つ．

（2） 任意の $a_1, a_2, \cdots, a_n \in R$ に対し，$a \in R$ で $a \equiv a_i \,(\mathrm{mode}\ \mathfrak{a}_i)$ $(i = 1, 2, \cdots, n)$ となるものが存在する (Chinese Remainder Theorem).

（3） $\mathfrak{a} = \bigcap_{1 \leqq i \leqq n} \mathfrak{a}_i$ とおくと $R/\mathfrak{a} \simeq (R/\mathfrak{a}_1) \oplus (R/\mathfrak{a}_2) \oplus \cdots \oplus (R/\mathfrak{a}_n)$ なる環の同型が成り立つ.

[証明] （1） $1 \leqq i \leqq n$ とする．このとき仮定より $u_j + v_j = 1$, $u_j \in \mathfrak{a}_i$, $v_j \in \mathfrak{a}_j$ ($\forall j \neq i$) なるものが存在する．そこで，$\prod_{j \neq i} (u_j + v_j) = 1$ なる積の左辺を展開し，$u_1, u_2, \cdots, u_n$ を含む積をまとめて $u_i{}^*$ とし，残りの $\prod_{j \neq i} v_j$ を $v_i{}^*$ とする．$\mathfrak{a}_1, \mathfrak{a}_2, \cdots, \mathfrak{a}_n$ は両側イデアルだから，$u_i{}^* \in \mathfrak{a}_i$, $v_i{}^* \in \bigcap_{j \neq i} \mathfrak{a}_j$, $u_i{}^* + v_i{}^* = 1$ となる．よって $\mathfrak{a}_i + \bigcap_{j \neq i} \mathfrak{a}_j = R$ となる.

（2） $u_i{}^*, v_i{}^*$ を（1）のようにし，$a_1, a_2, \cdots, a_n$ を R の任意の元とする．このとき $a = a_1 v_1{}^* + a_2 v_2{}^* + \cdots + a_n v_n{}^*$ とおくと，これは $a \equiv a_i v_i{}^* \equiv a_i \pmod{\mathfrak{a}_i}$ を満たす.

（3） $f : R \ni a \longmapsto (a + \mathfrak{a}_1, a + \mathfrak{a}_2, \cdots, a + \mathfrak{a}_n) \in (R/\mathfrak{a}_1) \oplus (R/\mathfrak{a}_2) \oplus \cdots \oplus (R/\mathfrak{a}_n)$ とおく．$\mathfrak{a}_1, \mathfrak{a}_2, \cdots, \mathfrak{a}_n$ は両側イデアルだから，これは環の準同型となる．また（2）より，f は全射であり，$\mathrm{Ker}(f) = \bigcap \mathfrak{a}_i = \mathfrak{a}$ である．よって準同型定理より，求める同型を得る. （証明終）

R が可換環のとき，R のイデアル $\mathfrak{a}, \mathfrak{b}$ が，$\mathfrak{a} + \mathfrak{b} = R$ を満たすなら，$\mathfrak{a}$ と $\mathfrak{b}$ は **互いに素** であるという.

例 1.9 $R = \boldsymbol{Z}$ とし，$\mathfrak{a}, \mathfrak{b}$ を R のイデアルとする．R のイデアルは，加群 $\boldsymbol{Z}$ の部分群だから，第Ⅱ章，§1，例 1.2 より $\mathfrak{a} = m\boldsymbol{Z}$, $\mathfrak{b} = n\boldsymbol{Z}$ $(m, n \in \boldsymbol{Z})$ と書ける．このとき，$\mathfrak{a}$ と $\mathfrak{b}$ が互いに素となるための必要十分条件は，$am + bn = 1$ となる $a, b \in \boldsymbol{Z}$ が存在することであり，また，m と n の素因数分解が，共通の素因数をもたぬことでもある．いずれにしても，$m\boldsymbol{Z}$ と $n\boldsymbol{Z}$ が互いに素なら，問題 1.3 と命題 1.8 より，$\boldsymbol{Z}/mn\boldsymbol{Z} \simeq \boldsymbol{Z}/m\boldsymbol{Z} \oplus \boldsymbol{Z}/n\boldsymbol{Z}$ となる．これは，第Ⅱ章，§5 の命題 5.4 の（1）の別証を与える.

§2. 素イデアルと極大イデアル

以下第Ⅲ章の終りまで，とくに断らない限り，可換環のみを扱う.

可換環 R で，R の 0 でない任意の元 a が逆元 a^{-1} をもつものを，体とよん

だ．命題1.1より，可換環Rが体となるための必要十分条件は，$R \supsetneqq \mathfrak{a} \supsetneqq \{0\}$なる$R$のイデアル$\mathfrak{a}$が存在しないことである．

Rを可換環とし，$\mathfrak{m}$をRのイデアルとする．もしRに$R \supsetneqq \mathfrak{a} \supsetneqq \mathfrak{m}$となるイデアル$\mathfrak{a}$が存在しないなら，$\mathfrak{m}$は**極大イデアル**であるという．

定理2.1 $\mathfrak{m}$を可換環Rのイデアルとする．このとき，$\mathfrak{m}$が極大イデアルとなるための必要十分条件は，剰余環$R/\mathfrak{m}$が体となることである．

[証明] 準同型定理より，$R \supsetneqq \mathfrak{a} \supsetneqq \mathfrak{m}$なる$R$のイデアル$\mathfrak{a}$と，$R/\mathfrak{m}$の$R/\mathfrak{m} \supsetneqq \mathfrak{a}' \supsetneqq \{0\}$なるイデアル$\mathfrak{a}'$とは1対1に対応する．よって，$R$が$R \supsetneqq \mathfrak{a} \supsetneqq \mathfrak{m}$なるイデアル$\mathfrak{a}$をもたないことは，$R/\mathfrak{m}$が体となることと同値である． (証明終)

極大イデアルの存在については，次の定理が成り立つ．

定理2.2 $\mathfrak{a}$を可換環Rのイデアルで，$\mathfrak{a} \neq R$とする．このとき，$\mathfrak{a}$を含むRの極大イデアルが存在する．

[証明]

$$\mathscr{B} = \{\mathfrak{b} \mid R \supsetneqq \mathfrak{b} \supset \mathfrak{a} \text{ なる } R \text{ のイデアル}\}$$

とおく．$\mathscr{B} \ni \mathfrak{a}$だから$\mathscr{B} \neq \emptyset$である．集合$\mathscr{B}$に順序を，

$$\mathfrak{b}_1 \geqq \mathfrak{b}_2 \iff R \text{ の部分集合とみて } \mathfrak{b}_1 \supset \mathfrak{b}_2$$

で入れる．$\mathscr{L}$を$\mathscr{B}$の全順序部分集合とし，$\mathfrak{l} = \bigcup_{\mathfrak{b} \in \mathscr{L}} \mathfrak{b}$とおく．$a, b \in \mathfrak{l}$とすると，$a \in \mathfrak{b}_1 \in \mathscr{L}$と$b \in \mathfrak{b}_2 \in \mathscr{L}$なる$\mathfrak{b}_1, \mathfrak{b}_2$が存在する．$\mathscr{L}$は全順序集合だから，$\mathfrak{b}_1 \supset \mathfrak{b}_2$か$\mathfrak{b}_1 \subset \mathfrak{b}_2$である．ところが$\mathfrak{b}_1, \mathfrak{b}_2$は$R$のイデアルだから，$a \pm b \in \mathfrak{b}_1$または$\in \mathfrak{b}_2$が成り立ち，$a \pm b \in \mathfrak{l}$となる．また$r \in R$とすると，$ra \in \mathfrak{b}_1$または$\in \mathfrak{b}_2$だから，$ra \in \mathfrak{l}$となる．よって$\mathfrak{l}$は$R$のイデアルである．また$\forall \mathfrak{b} \in \mathscr{L}$は$\mathfrak{a} \subset \mathfrak{b}$, $1 \notin \mathfrak{b}$を満たすから，$\mathfrak{a} \subset \mathfrak{l}$, $1 \notin \mathfrak{l}$も成り立ち，$\mathfrak{l} \in \mathscr{B}$となる．作り方より$\mathfrak{l}$は$\mathscr{L}$の上界を与えるから，$\mathscr{B}$は帰納的となる（第Ⅰ章，§3参照）．よってツォルンの補題より，$\mathscr{B}$は極大元$\mathfrak{m}$をもつ．明らかに$R \supsetneqq \mathfrak{m} \supset \mathfrak{a}$である．また，$\mathfrak{m}$は$\mathscr{B}$の極大元だから，$\mathfrak{m}$を真に含む$R$のイデアルは存在しない．よって$\mathfrak{m}$は極大イデアルである． (証明終)

$\mathfrak{p}$を可換環Rのイデアルで，$\mathfrak{p} \neq R$であるとする．このとき，$R/\mathfrak{p}$が整域となるなら，$\mathfrak{p}$は**素イデアル**であるという．このことは，$a \in R$が

$$a \notin \mathfrak{p},\ b \notin \mathfrak{p} \implies ab \notin \mathfrak{p}$$

となることを意味する．体は整域だから，極大イデアルは素イデアルである．

例 2.3　$R = \boldsymbol{Z}$とする．$\boldsymbol{Z}$は整域だが体ではないから，Rのイデアル $\{0\}$ は，素イデアルだが極大イデアルではない．mを2以上の整数とし，$\mathfrak{a} = m\boldsymbol{Z} = (m)$ とおく．このとき$\mathfrak{a}$が素イデアルとなるための必要十分条件は，第I章，例6.2より，mが素数となることである．しかも，mが素数なら$\boldsymbol{Z}/m\boldsymbol{Z}$は体となるから，$\mathfrak{a}$は極大イデアルにもなる．

問題 2.4　Rを（可換とは限らない）環とし，$\mathfrak{a}$を$\mathfrak{a} \subsetneqq R$なる左(右，両側)イデアルとする．このとき$\mathfrak{a}$を含む$R$の極大左(右，両側)イデアルが存在することを示せ．

問題 2.5　Rを可換環，$\mathfrak{a}, \mathfrak{b}$を$R$のイデアル，$\mathfrak{p}$を$R$の素イデアルとする．このとき $\mathfrak{a}\mathfrak{b} \subset \mathfrak{p}$ なら，$\mathfrak{a} \subset \mathfrak{p}$ または $\mathfrak{b} \subset \mathfrak{p}$ となることを示せ．

§3.　局所化と商体

Rを可換環とし，SをRの部分集合とする．Sが次の条件を満たすとき，SをRの **乗法的閉集合** という：

(MC 1)　　$a, b \in S \implies a \cdot b \in S,$

(MC 2)　　$1 \in S,\ 0 \notin S.$

例えば，Rの非零因子全体のなす集合や，$R \setminus \mathfrak{p} = \{a \in R \mid a \notin \mathfrak{p}\}$（$\mathfrak{p}$は$R$の素イデアル）は，乗法的閉集合をなす．

SをRの乗法的閉集合とし，積集合$R \times S$において，次のようにして同値関係を導入する：

$$(a_1, s_1) \sim (a_2, s_2) \iff \text{ある } s \in S \text{ に対し } (a_1 s_2 - a_2 s_1)s = 0.$$

Sは乗法的に閉じているから，この $\sim$ は実際に同値関係となり，$R \times S$の類別を定める．そこで (a, s) を含む類を a/s で表し，その全体を R_S または RS^{-1} と表す．

$a_1/s_1, a_2/s_2 \in R_S$ に対し，次のようにして和と積を定める：

$$(a_1/s_1) + (a_2/s_2) = (a_1 s_2 + a_2 s_1)/s_1 s_2,$$

$$(a_1/s_1)\cdot(a_2/s_2) = a_1a_2/s_1s_2.$$

これは，整数環 $\boldsymbol{Z}$ より有理数体 $\boldsymbol{Q}$ を作る作り方を一般化したものである．

命題 3.1 上の R_S の和 $(a_1/s_1)+(a_2/s_2)$ と積 $(a_1/s_1)\cdot(a_2/s_2)$ は，同値類 $a_1/s_1, a_2/s_2$ より代表 $(a_1, s_1), (a_2, s_2)$ のとり方によらず，一意的に定まる．さらに，このようにして定義した和と積に関し，R_S は，0/1 を零元，1/1 を単位元とする可換環をなす．この R_S を，R の S による **商環**（または **局所化**）とよぶ．

［証明］ $a_1/s_1 = a_1'/s_1'$, $a_2/s_2 = a_2'/s_2'$ とし，$s, t \in S$ が $(a_1s_1' - a_1's_1)s = 0$, $(a_2s_2' - a_2's_2)t = 0$ を満たすとする．このとき，

$$\begin{aligned}&\{(a_1s_2 + a_2s_1)s_1's_2' - (a_1's_2' + a_2's_1')s_1s_2\}st\\ &\qquad = (a_1s_1' - a_1's_1)s(s_2s_2't) + (a_2s_2' - a_2's_2)t(s_1s_1's) = 0\end{aligned}$$

が成り立つから，

$$(a_1/s_1) + (a_2/s_2) = (a_1'/s_1') + (a_2'/s_2')$$

が成り立ち，和は一意的に定まっている．積についても同様である．

環の公理を満たすことも，

$$\begin{aligned}(a_1/s_1)\{(a_2/s_2) + (a_3/s_3)\} &= (a_1/s_1)\{(a_2s_3 + a_3s_2)/s_2s_3\}\\ &= (a_1a_2s_3 + a_1a_3s_2)/s_1s_2s_3 = (a_1a_2/s_1s_2) + (a_1a_3/s_1s_3)\end{aligned}$$

等のようにして，容易に証明される．（証明終）

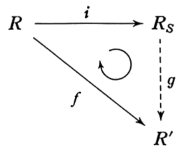
R_S を R の S による商環とし，写像

$$i: \quad R \ni a \longmapsto (a/1) \in R_S$$

を考える．これが環の準同型となることは，R_S での演算の定義より明らかである．またこの写像による $S \subset R$ の像は，$i(S) = \{(s/1) \mid s \in S\}$ であり，その元 $i(s) = s/1$ は逆元 $1/s$ をもち単数となる．次の定理は，商環 R_S が，この性質をもつ最も一般的な環であることをいっている．

定理 3.2 S を可換環 R の乗法的閉集合とし，R_S を R の S による商環とする．$f: R \longrightarrow R'$ を可換環の準同型で，$f(S)$ が R' の単数のなす群 $U(R')$ に写されるものとする．このとき準同型 $g: R_S \longrightarrow R'$ で，$f = g \circ i$ を満たす

ものが唯一つ存在する．これを **商環の普遍性** とよぶ．



[証 明]　g が存在すれば，

$$g(a/s) = g((a/1)\cdot(s/1)^{-1}) = g(i(a))g(i(s))^{-1}$$
$$= f(a)f(s)^{-1}$$

が成り立つから，このような g は一意的に定まる．

R_S の任意の元は a/s $(a \in R,\ s \in S)$ と書けるから，$g(a/s) = f(a)f(s)^{-1}$ とおく．仮定 $f(S) \subset U(R')$ より，$f(s) \in U(R')$ は逆元をもつから，$f(a)f(s)^{-1}$ は意味をもつ．また $a/s = a'/s'$ とし，$t \in S$ が $(as' - a's)t = 0$ を満たすとすれば，$(f(a)f(s') - f(a')f(s))f(t) = 0$ となる．ところが，$f(s), f(s'), f(t)$ は R' の単数だから，この式を $f(s)f(s')f(t)$ で割り整理すると，$f(a)f(s)^{-1} = f(a')f(s')^{-1}$ となる．よって $g(a/s)$ は，a/s の代表元 (a, s) のとり方によらずに定まっている．

g が環の準同型となることは，f が環の準同型であることより，容易に確かめられる．さらに

$$g(i(a)) = g(a/1) = f(a)f(1)^{-1} = f(a)$$

だから，可換性 $f = g \circ i$ も成り立つ．　　　　（証明終）

S として，可換環 R の非零因子の全体をとったとき，これより作られる R_S を **全商環** とよび，$Q(R)$ とも表す．この場合

$$(a_1, s_1) \sim (a_2, s_2) \iff a_1 s_2 = a_2 s_1$$

となっており，写像 $i : R \longrightarrow R_S$ は単射となる．したがって，R は R_S の部分環と思え，$a \in R$ と $a/1$ を同一視すると，

$$R_S = \{as^{-1} \mid a \in R,\ s \in S\}$$

と書ける．とくに R が整域のときは，R の 0 でない元がすべて非零因子となるから，$S = R\setminus\{0\}$ となる．よって，R_S の 0 でない元 ab^{-1} $(S \ni a, b \neq 0)$ は逆元 ba^{-1} をもち，R_S は体となる．これを整域 R の **商体** とよぶ．

例 3.3　(1)　有理数体 $\boldsymbol{Q}$ は，整数環 $\boldsymbol{Z}$ の商体である．

(2)　R を整域，K を R の商体とする．このとき，多項式環 $R[x_1, x_2, \cdots, x_n]$ は整域

となり，その商体を $K(x_1, x_2, \cdots, x_n)$ で表し，（K を係数とする）$x_1, x_2, \cdots, x_n$ の **有理関数体** とよぶ．また $K(x_1, x_2, \cdots, x_n)$ の元を **有理関数** とよぶ．

$\mathfrak{p}$ を可換環 R の素イデアルとすると，$S = R \setminus \mathfrak{p}$ は乗法的閉集合となる．このSによる R の商環 R_S を $R_\mathfrak{p}$ で表し，R の $\mathfrak{p}$ における **局所化** とよぶ．

一般に，極大イデアルがただ一つしか存在しない可換環を **局所環** とよぶ．R を局所環，$\mathfrak{m}$ をその極大イデアルとするとき，$R/\mathfrak{m}$ を **剰余体** とよぶ．上記の局所化 $R_\mathfrak{p}$ は，次の命題より，局所環であることがわかる．

命題 3.4　R を可換環とするとき，R が局所環となるための必要十分条件は，R の非単数の全体 $R \setminus U(R)$ がイデアルをなすことである．

［証明］（必要性）　$\mathfrak{m}$ を R の唯一つの極大イデアルとする．$U(R)$ の元 u は $Ru = R$ を満たすから，$\mathfrak{m} \subsetneqq R$ は u を含まず，したがって，$R \setminus U(R) \supset \mathfrak{m}$ である．ところが $R \setminus U(R)$ の元 a は，単数でないから $Ra \subsetneqq R$ となる．よって，定理 2.2 より，Ra は R の極大イデアル $\mathfrak{m}$ に含まれる．したがって $R \setminus U(R) \subset \mathfrak{m}$ が成り立つ．よって $R \setminus U(R) = \mathfrak{m}$ となり，$R \setminus U(R)$ はイデアルとなる．

（十分性）　$R \setminus U(R)$ がイデアルであるとし，これを $\mathfrak{m}$ で表す．$1 \notin \mathfrak{m}$ より $\mathfrak{m} \subsetneqq R$ である．$R \supsetneqq \mathfrak{a}$ なる任意のイデアル $\mathfrak{a}$ をとる．$U(R)$ の元 u は $Ru = R$ を満たすから，$R \setminus U(R) \supset \mathfrak{a}$ である．よって $\mathfrak{m} \supset \mathfrak{a}$ だから，$\mathfrak{m}$ は R の唯一つの極大イデアルである．

（証明終）

定理 3.5　$\mathfrak{p}$ を可換環 R の素イデアルとすると，局所化 $R_\mathfrak{p}$ は局所環で，$\mathfrak{m} = \{a/s \mid a \in \mathfrak{p},\ s \notin \mathfrak{p}\}$ がその唯一つの極大イデアルとなる．

［証明］　$R_\mathfrak{p}$ において a/s $(a, s \in R,\ s \notin \mathfrak{p})$ が単数であったとする．b/t がその逆元だとすると，$ab/st = 1$ となる．よって $u \in R$, $u \notin \mathfrak{p}$ があり，$(ab - st)u = 0$ となる．$\mathfrak{p}$ は素イデアルで，$abu = stu \notin \mathfrak{p}$ だから，$a \notin \mathfrak{p}$ となる．逆に $a \notin \mathfrak{p}$ なら $s/a \in R_\mathfrak{p}$ が a/s の逆元を与える．よって

$$U(R_\mathfrak{p}) = \{a/s \mid a, s \in R,\ a, s \notin \mathfrak{p}\}$$

である．したがって $R_\mathfrak{p} \setminus U(R_\mathfrak{p}) = \mathfrak{m}$ となる．$\mathfrak{m}$ は明らかに $R_\mathfrak{p}$ のイデアルとなるから，前命題より，$R_\mathfrak{p}$ は局所環となる．　　　　（証明終）

例 3. 6　R を可換環とするとき，文字 x を含む

$$f(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_m x^m + \cdots \qquad (a_0, a_1, a_2, \cdots, a_m, \cdots \in R)$$

の形の式全体を $R[[x]]$ で表し，R を係数とする x の **形式的べき級数環** とよぶ．これは，多項式環の定義と非常に似ているが，多項式環の場合に必要な，「m が十分大なら $a_m = 0$」という条件を除いている．$R[[x]]$ での和と積は，$R[x]$ の場合と同様に定義され，$R[[x]]$ は可換環となる．多変数の形式的べき級数環 $R[[x_1, x_2, \cdots, x_n]]$ も，多項式環 $R[x_1, x_2, \cdots, x_n]$ と同様に，

$$R[[x_1, x_2, \cdots, x_n]] = R[[x_1, x_2, \cdots, x_{n-1}]][[x_n]]$$

として定義される．

$f(x) = \sum_{0\leq m<\infty} a_m x^m$ と $g(x) = \sum_{0\leq m<\infty} b_m x^m$ を $R[[x]]$ の元とする．このとき

$$f(x)g(x) = \sum_{0\leq m<\infty} \left(\sum_{l+n=m} a_l b_n\right) x^m$$

である．よって $\{a_m\}$ のうち 0 でない最初のものを a_s とし，$\{b_m\}$ のうち 0 でない最初のものを b_t とすると，

$$f(x)g(x) = a_s b_t x^{s+t} + (x \text{ の } (s+t+1) \text{ 次以上の項})$$

となる．よって，R が整域なら，$R[[x]]$ も整域となる．

R が体 K であるとし，

$$K[[x]] \ni f(x) = \sum a_m x^m \longmapsto f(0) = a_0 \in K$$

なる写像を考える．これは環 $K[[x]]$ より体 K への全射な準同型である．よって，この写像の核

$$\mathfrak{m} = \{f(x) \in K[[x]] \mid f(0) = 0\}$$

は，$K[[x]]$ の極大イデアルである．

$\mathfrak{m}$ が $K[[x]]$ の唯一つの極大イデアルであることを示すため，$f(x) = \sum a_m x^m \in K[[x]]$ が $f(0) = a_0 \neq 0$ であるとする．このとき $g(x) = \sum b_m x^m$ が，$f(x)g(x) = 1$ を満たすための必要十分条件は

$$a_0 b_0 = 1, \qquad \sum_{l+n=m} a_l b_n = 0 \qquad (\forall m \geqq 1)$$

である．ところが $a_0 \neq 0$ は，体 K において逆元 a_0^{-1} をもつから，$b_0 = a_0^{-1}$ とおき，b_1, $b_2, \cdots$ を順に

$$b_m = -a_0^{-1}(a_m b_0 + a_{m-1} b_1 + \cdots + a_1 b_{m-1})$$

なる式で定めればよい．したがって，$f(x) \in K[[x]]$ が $\mathfrak{m}$ に入らないなら，$f(x)$ は $K[[x]]$ 内に逆元をもつ．よって命題 3.4 より，$K[[x]]$ は局所環で，$\mathfrak{m}$ はその唯一つ

の極大イデアルとなる.

問題 3. 7　Kを体とする. 形式的べき級数環 $K[[x]]$ の商体を求めよ.

問題 3. 8　Kを体とするとき, 形式的べき級数環 $K[[x_1, x_2, \cdots, x_n]]$ は局所環であることを示せ.

§4. 一意分解環

4. 1　一意分解環　Rを整域とし, Kを商体とする. この節では, 整数環 $\boldsymbol{Z}$ における素因数分解の一般化を行う.

Rの2元 $a, b\ (\neq 0)$ に対し, $a = bc$ となる $c \in R$ が存在することと, 単項イデアル $(a), (b)$ の間に $(a) \subset (b)$ なる関係があることとは同値である. このとき $b|a$ と書き, bはaを **割り切る**, bはaの **約数** である, aはbの **倍数** である, などという.

$a|b$ かつ $b|a$ とする. このとき $a = bc$, $b = ad$ $(\exists c, d \in R)$ となるから, $a = a(cd)$ となる. Rは整域だから, $cd = 1$ となり, c, d はRの単数となる. したがって,

$$a|b \quad \text{かつ} \quad b|a \iff a = b\varepsilon \ (\exists \varepsilon \in U(R)) \iff (a) = (b)$$

が成り立つ. このとき, aとbは **同伴** であるといい, $a \approx b$ と表す.

$a \in R$ が0でも単数でもないものとする. このとき, 任意のRの単数εに対し, $a\varepsilon | a$ および $\varepsilon | a$ となることは明らかであるが, 逆にRの元pの約数がこの様なものに限るとき, pは **素元** であるという. いい直すと, pがRの素元であることは,

$$p = ab \ (a, b \in R) \implies a \text{ または } b \text{ が単数}$$

となることをいう.

命題 4. 1　pを整域Rの0でない元とする. もし単項イデアル (p) が素イデアルであるなら, pは素元である.

［証 明］ $p=ab$ $(a,b\in R)$ とする．(p) は素イデアルだから，$ab\in(p)$ より $a\in(p)$ または $b\in(p)$ が成り立つ．第1の場合は，$a=pc$ $(c\in R)$ と書くと，$bc=1$ となり，$b\in U(R)$ となる．第2の場合は $a\in U(R)$ となる．　（証明終）

$a_1,a_2,\cdots,a_n$ を R の0でない元とする．もし $0\neq d\in R$ が $d|a_i$ $(i=1,2,\cdots,n)$ を満たすなら，d は $\{a_i\}$ の **公約数** であるという．また $0\neq m\in R$ が $a_i|m$ $(i=1,2,\cdots,n)$ を満たすなら，m は $\{a_i\}$ の **公倍数** であるという．$\{a_i\}$ のある公約数 d が，任意の a_i の公約数の倍数となるなら，d は $\{a_i\}$ の **最大公約数** であるという．**最小公倍数** も同様に定義される．最大公約数や最小公倍数は，一般には存在するとは限らないが，もし存在すれば，単数の差を除いて一意的に定まる．また，R が以下のべる一意分解環の場合は，これらは存在することがわかる．

R を整域とする．このとき次の **(UF 1)**, **(UF 2)** が成り立つなら，R は **一意分解環** であるという：

(UF 1)　a を R の0でも単数でもない元とする．このとき a は，$a=p_1p_2\cdots p_s$（p_i は素元）の形に書ける．

(UF 2)　$a=p_1p_2\cdots p_s=q_1q_2\cdots q_t$ を a の素元の積としての2つの表示とする．このとき $s=t$ であり，さらに番号をつけ直すことにより，$p_1\approx q_1$，$p_2\approx q_2,\cdots,p_s\approx q_s$ が成り立つ．

R を一意分解環とし，R の素元全体の集合を同伴という関係で類別し，完全代表系 P をとる．このとき，R の0でない元 a は，

$$a=up_1^{e_1}p_2^{e_2}\cdots p_s^{e_s}\qquad (u\text{ は単数},\ p_i\in P,\ e_i\in \boldsymbol{N})$$

の形に一意的に表される．

命 題 4. 2　R を一意分解環とし，p を R の0でない元とする．このとき p が素元となるための必要十分条件は，(p) が素イデアルとなることである．

［証 明］ 十分性は命題4.1である．必要性を示すため，p を素元とし，$ab\in(p)$ とする．このとき $ab=cp$ $(c\in R)$ と書ける．この右辺の素元分解には p が現れるから，

素元分解の一意性より，a, b の素元分解のうちどちらかには，p と同伴な数が現れる．よって $a \in (p)$，または $b \in (p)$ が成り立つ． (証明終)

問題 4.3 Rを一意分解環，PをRの素元の完全代表系，$a = up_1^{e_1}p_2^{e_2}\cdots p_s^{e_s}$，$b = vp_1^{f_1}p_2^{f_2}\cdots p_s^{f_s}$ ($u, v \in U(R)$，$p_i \in P$，$0 \leqq e_i, f_i \in \boldsymbol{Z}$) とする．このとき次のことを示せ：

(1) $a|b \iff e_i \leqq f_i \quad (i = 1, 2, \cdots, s)$.

(2) $d_i = \min(e_i, f_i)$，$m_i = \max(e_i, f_i)$ とおくと，a, b の最大公約数は $p_1^{d_1}p_2^{d_2}\cdots p_s^{d_s}$ で，最小公倍数は $p_1^{m_1}p_2^{m_2}\cdots p_s^{m_s}$ である．

4.2 単項イデアル整域 整域Rにおいて，任意のイデアルが単項イデアルとなるとき，Rを**単項イデアル整域**とよぶ．このとき次の定理が成り立つ．

定理 4.4 単項イデアル整域は一意分解環である．

定理の証明のため次の補題を証明する．

補題 4.5 Rを単項イデアル整域，$0 \neq p \in R$とする．このとき次は同値である．

(1) pは素元である．

(2) $p|ab \ (a, b \in R) \implies p|a$ または $p|b$.

(3) (p) は素イデアルである．

(4) (p) は極大イデアルである．

[補題 4.5 の証明] (2) は (3) をいい直したものにすぎない．

(1) $\Longrightarrow$ (4) pを素元とし，$(p) \subset (a) \subsetneqq R$とする．$p \in (a)$ だから，$p = ab$ と書け，$(a) \neq R$ だから $a \notin U(R)$ である．よって (1) より $b \in U(R)$ となり，$(p) = (a)$ となる．よって (p) は極大イデアルである．

(4) $\Longrightarrow$ (3) 極大イデアルは素イデアルである．

(3) $\Longrightarrow$ (1) これは命題 4.1 で示した． (証明終)

[定理 4.4 の証明] **(UF 1)**．a_0 はRの0でも単数でもない元で，**(UF 1)** が成り立

たぬものとする．a_0 は素元でないから，$b_1, c_1 \in R$ で，$b_1, c_1 \notin U(R)$ かつ $a_0 = b_1c_1$ となるものが存在する．b_1, c_1 の双方について (**UF 1**) が成り立つなら，$a_0 = b_1c_1$ についても (**UF 1**) が成り立つ．したがって，b_1 または c_1 について (**UF 1**) が成り立たないが，それを a_1 とおく．$b_1, c_1 \notin U(R)$ だから，$(a_0) \subsetneqq (a_1)$ である．a_1 について同じことを繰り返して a_2 を作り，さらに同じことを繰り返し，

$$(a_0) \subsetneqq (a_1) \subsetneqq (a_2) \subsetneqq \cdots \subsetneqq (a_n) \subsetneqq \cdots$$

なる R のイデアルの無限増加列を作る．このとき和集合 $\bigcup_{n\geq 0} (a_n)$ は R のイデアルをなす．ここで R は単項イデアル整域だから，$\bigcup_{n\geq 0} (a_n) = (a)$ と書ける．このとき a はある (a_n) に属するが，そうすると，$(a_{n+1}) \subset (a) \subset (a_n)$ となり，$(a_n) = (a_{n+1})$ となる．これは矛盾である．

(**UF 2**)． $a = p_1p_2\cdots p_s = q_1q_2\cdots q_t$ を a の素元の積としての表示とし，(**UF 2**) を s に関する帰納法で示す．p_s は素元だから，補題の (2) より，$p_s | q_1q_2\cdots q_t$ から $p_s | q$ $(1 \leqq \exists i \leqq t)$ が従う．q の番号をつけ直し，それを q_t だとする．このとき $(q_t) \subset (p_s)$ となるが，q_t も素元だから (p_s) も (q_t) も極大イデアルとなり，$(p_s) = (q_s)$ となる．したがって，$q_s = p_su$ $(\exists u \in U(R))$ となるが，このとき $p_1p_2\cdots p_{s-1} = q_1q_2\cdots(q_{t-1}u)$ となる．よって帰納法の仮定より，$s-1 = t-1$，かつ q の番号をつけ直すと $p_1 \approx q_1$，$p_2 \approx q_2, \cdots$，$p_{s-1} \approx q_{t-1}u \approx q_{t-1}$ が成り立つ． (証明終)

(注) 定理の証明より，R がネター環（次節参照）なら (**UF 1**) が成り立つことがわかる．ネター環でも一意分解環とならないものは沢山あるから，一見成り立ちそうに見える (**UF 2**) の方が，(**UF 1**) より成り立ちにくい．

例 4. 6 R を整域とするとき，R から整列集合 W (第 I 章，§3 参照) への写像 $\varphi: R \longrightarrow W$ で，次の性質を満たすものが存在するとき，R を **ユークリッド環** という：

(**E 1**) W の最小元を w_0 とすると，$\varphi(a) = w_0 \iff a = 0$.

(**E 2**) $a, b \in R$, $b \neq 0$ なら

$$a = qb + r, \qquad \varphi(r) < \varphi(b)$$

を満たす $q, r \in R$ が存在する．

$\mathfrak{a}$ をユークリッド環 R のイデアル，$\neq \{0\}$ とし，W の部分集合 $\{\varphi(a) \mid 0 \neq a \in \mathfrak{a}\}$ の最小値が $\varphi(a_0)$ $(0 \neq a_0 \in \mathfrak{a})$ だとする．a を $\mathfrak{a}$ の任意の元とし，$a = qa_0 + r$, $\varphi(r) < \varphi(a_0)$ となる $q, r \in R$ をとる．$r = a - qa_0 \in \mathfrak{a}$ かつ $\varphi(r) < \varphi(a_0)$ であるから，$\varphi(a_0)$ の最小性より $r = 0$ となる．よって $a = qa_0$ となり，$\mathfrak{a} = (a_0)$ となる．したが

って，ユークリッド環は単項イデアル整域となる．

次の (1),(2) は，ユークリッド環の代表的な例である：

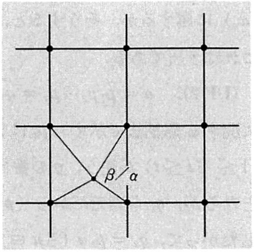
(1) $R=\boldsymbol{Z},\ W=\{0\}\cup\boldsymbol{N},\ \varphi(a)=|a|$ (絶対値).

(2) Rを体K上の一変数多項式環，$W=\{-\infty\}\cup\{0\}\cup\boldsymbol{N}$,

$$\varphi:\quad K[x]\ni f(x)\ \longmapsto\ \deg f(x)\in\{-\infty\}\cup\{0\}\cup\boldsymbol{N}.$$

ユークリッド環は単に単項イデアル整域であるだけでなく，単項イデアルの生成元や最大公約数などが，具体的に計算できる点において重要である．

問題 4.7 $R=\{\alpha\in\boldsymbol{C}\mid\alpha=a+b\sqrt{-1},\ a,b\in\boldsymbol{Z}\}$ をガウスの整数環とよぶ．$\alpha=a+b\sqrt{-1}$に対し，$\varphi(\alpha)=a^2+b^2$とおく．$\alpha,\beta\in R,\ \alpha\neq 0$に対し，$\beta/\alpha=c+d\sqrt{-1}$ $(c,d\in\boldsymbol{R})$ とおき，c,dに最も近い整数をm,nとする．$q=m+n\sqrt{-1},\ r=\beta-q\alpha$とおくと，$\varphi(r)<\varphi(\alpha)$ となることを示し，Rがユークリッド環となることを示せ．



4.3 多項式環での既約性

以下次の定理を証明する．

定理 4.8 Rが一意分解環なら，多項式環 $R[x_1,x_2,\cdots,x_n]$ も一意分解環である．

Rを整域とし，$f(x)\in R[x]$ は定数ではないものとする．このとき，$f(x)$ が $R[x]$ において

$$f(x)=g(x)h(x),\qquad \deg g(x)>0,\ \deg h(x)>0$$

と分解されるなら，$f(x)$ は **可約** であるといい，そうでないとき **既約** であるという．Rが体Kなら，$U(K[x])=K\setminus\{0\}$ となるから，$f(x)$ が既約となるための必要十分条件は，$f(x)$ が$K[x]$ の素元となることである．

Rを一意分解環とし，Kをその商体とする．このとき第Ⅰ章，定理9.1より，$K[x]$ はユークリッド環（例4.6参照）となる．よって定理4.4により，$K[x]$ は一意分解環となる．

R の元 a,b は，その最大公約数が 1 となるとき，**互いに素**であるという．また R 上の多項式 $f(x)=a_0+a_1x+\cdots+a_mx^m$ は，係数 $a_0,a_1,\cdots,a_m$ の最大公約数が 1 となるとき，**原始多項式**であるという．

補題 4.9 R,K を上のようにするとき，$f(x)\in K[x]$ は $c\in K$ と原始多項式 $f_0(x)\in R[x]$ があり，$f(x)=cf_0(x)$ と書ける．しかも，c は R の単数の差を除いて，$f(x)$ により一意的に定まる．このような c を一つとり，$c=I(f)$ とおき，$f(x)$ の**内容**とよぶ．

[証明] (存在). $f(x)=c_0+c_1x+\cdots+c_mx^m$ $(c_i\in K)$
とする．K は R の商体だから $c_i=a_i/b_i$ $(a_i,b_i\in R)$ と書ける．$b=b_0b_1\cdots b_m$ とおくと，$bf(x)$ の係数 bc_i は R に属す．そこで $bc_0,bc_1,\cdots,bc_m$ の最大公約数を a とおき，

$$c=a/b,\qquad bc_i=ac_i'\ (c_i'\in R),\qquad f_0(x)=c_0'+c_1'x+\cdots+c_m'x^m$$

とおくと，$f(x)=cf_0(x)$ で，$f_0(x)$ は原始多項式となる．

(一意性). $f(x)=cf_0(x)=c'f_0'(x)$ を補題のような 2 つの表現とする．K は一意分解環 R の商体だから，$c=a/b,\ c'=a'/b'$ $(a,b,a',b'\in R,\ a$ と $b,\ a'$ と b' は互いに素$)$ と書く．このとき

$$ab'f_0(x)=a'bf_0'(x)\in R[x]$$

となるが，$f_0(x),f_0'(x)$ は原始多項式だから，左辺の係数の最大公約数は ab'，右辺の係数の最大公約数は $a'b$ となる．よって $ab'\approx a'b$ となるが，a と b，a' と b' は互いに素だから，$a\approx a'$，$b\approx b'$ となる． (証明終)

補題 4.10 (ガウスの補題) R,K を前の通りとすると，

(1) 原始多項式の積はまた原始多項式である．

(2) $I(fg)$ と $I(f)I(g)$ は R の単数の差を除いて等しい．

[証明] 前補題のように，$f(x)=I(f)f_0(x)$，$g(x)=I(g)g_0(x)$ と書くとき，$f(x)g(x)=I(f)I(g)f_0(x)g_0(x)$ が成り立つから，補題の (2) は (1) より従う．

(1) を示すため，$f(x),g(x)\in R[x]$ が原始多項式であるとする．積 $f(x)g(x)$ が原始多項式ではないとすると，その係数の最大公約数 d は 1 でない．よって p を d を割る素元とすると，$f(x)g(x)$ の係数はすべて p で割り切れる．ところが $f(x),g(x)$ は原始多項式だから，p で割れない係数が存在する．そこで

$$f(x) = a_0 + a_1 x + \cdots + a_m x^m, \qquad g(x) = b_0 + b_1 x + \cdots + b_n x^n$$

とし，a_s と b_t を p で割れない $f(x)$ と $g(x)$ の最初の係数とする．このとき $f(x)g(x)$ の x^{s+t} の係数は，

$$(a_0 b_{s+t} + a_1 b_{s+t-1} + \cdots + a_{s-1} b_{t+1}) + a_s b_t + (a_{s+1} b_{t-1} + a_{s+2} b_{t-2} + \cdots + a_{s+t} b_0)$$

となり，この第1項では a_i が p で割れ，第3項では b_j が p で割れる．ところが $a_s b_t$ は p で割れないから，x^{s+t} の係数は p で割れない．これは矛盾である． (証明終)

この補題より，次の系が導かれる．

系 4. 11 R, K を前の通りとする．このとき，$R[x]$ の既約多項式は，$K[x]$ においても既約である．

[系 4.11 の証明] $f(x) \in R[x]$ が $K[x]$ において $f(x) = g(x)h(x)$，$\deg g(x) > 0$，$\deg h(x) > 0$ と分解されたとする．補題 4.9 より，$f(x) = I(f)f_0(x)$，$g(x) = I(g)g_0(x)$，$h(x) = I(h)h_0(x)$ と，K の元と原始多項式の積に書く．ガウスの補題により，$I(f) = I(g)I(h)u$ $(\exists u \in U(R))$ が成り立つから，$f(x) = I(f)u^{-1}g_0(x)h_0(x)$ となる．よって $f(x)$ は $R[x]$ でも既約でない． (証明終)

[定理 4.8 の証明] 帰納法により，$n=1$ のときに示せばよいから，R を一意分解環としたとき，$R[x]$ も一意分解環となることを示す．

$$\deg\{g(x)h(x)\} = \deg g(x) + \deg h(x)$$

が成り立つから，$R[x]$ の元 $g(x)$ が R の 0 でない元を割るなら，$g(x)$ も R の元となる．これより $U(R[x]) = U(R)$ であり，また R の素元は $R[x]$ でも素元となることがわかる．

そこで，原始多項式 $f_0(x)$ が既約で，かつ $f_0(x) = g(x)h(x)$ と $R[x]$ で積になったとする．このとき，$g(x)$ または $h(x)$ は R の元となり，ガウスの補題より，それは R の単数となる．よって既約な原始多項式は，$R[x]$ の素元となる．補題 4.9 より，$R[x]$ の素元はこの2種類に限る．

(UF 1). $f(x)$ を $R[x]$ の 0 でない元とする．補題 4.9 より，$f(x) = I(f)f_0(x)$ ($I(f) \in R$，$f_0(x)$ は原始多項式) と書ける．R は一意分解環だから，$I(f) = p_1 p_2 \cdots p_s$ と $I(f)$ は R の素元の積に表される．また $f_0(x)$ は，一意分解環 $K[x]$ において，$f_0(x) = q_1(x)q_2(x)\cdots q_t(x)$ と既約多項式の積に分解できる．そこで $q_j(x)$ を補題 4.9 のように分解すると，ガウスの補題より，$I(q_1(x))I(q_2(x))\cdots I(q_t(x)) \approx I(f_0(x)) = 1$ と

なる．そこで $I(q_j(x))^{-1}q_j(x)\in R[x]$ を改めて $q_j(x)$ とおくことにより，$q_j(x)$ ($\forall j=1,2,\cdots,t$) は $R[x]$ の既約な原始多項式であるとしてよい．このとき，p は R の素元だから，$R[x]$ でも素元である．また，$q_j(x)$ は既約な原始多項式だから，$R[x]$ の素元である．よって $f(x)=p_1p_2\cdots p_sq_1(x)q_2(x)\cdots q_t(x)$ は素元分解を与える．

(UF 2)．$f(x)=p_1p_2\cdots p_sq_1(x)q_2(x)\cdots q_t(x)=p_1'p_2'\cdots p_{s'}'q_1'(x)q_2'(x)\cdots q_{t'}'(x)$ を $R[x]$ での2つの素元分解とし，$p_i, p_i'\in R$, $\deg q_j(x)$，$\deg q_j'(x)>0$ とする．$q_j(x)$ と $q_j'(x)$ は $R[x]$ で既約だから，$K[x]$ でも既約となる．よって上の2つの分解を一意分解環 $K[x]$ での素元分解と思うと，$t'=t$ であり，かつ順番をつけ直すと，$q_j'(x)=c_jq_j(x)$ ($\exists c_j\in K$) となる．ところが $q_j(x)$ も $q_j'(x)$ も原始多項式だから，$c_j\in U(R)$ となる．よって $u=c_1c_2\cdots c_t\in U(R)$，$p_1p_2\cdots p_s=up_1'p_2'\cdots p_{s'}'$ となる．

ここで p_i と p_i' は R の素元だから，R での一意性より，$s'=s$ であり，また順番をつけ直すと，$p_1'\approx p_1$，$p_2'\approx p_2$，$\cdots$，$p_s'\approx p_s$ となる．（証明終）

4. 4 離散的付値環* K を体とする．このとき，写像 $\varphi: K\longrightarrow\{r\in \boldsymbol{R}\mid r\geqq 0\}$ で，次の条件を満たすものを（乗法）**付値** とよぶ：

(MV 0) $\varphi(a)=0 \iff a=0$,

(MV 1) $\varphi(ab)=\varphi(a)\varphi(b)$,

(MV 2) $\varphi(a+b)\leqq\varphi(a)+\varphi(b)$.

(MV 2) は，$x,y\in K$ に対し

$$d(x,y)=\varphi(x-y)$$

とおくと，d は K の距離となることをいっている．φ が **(MV 2)** より強い条件

(MV 2′) $\varphi(a+b)\leqq\max(\varphi(a),\varphi(b))$

を満たすとき，φ は **非アルキメデス的付値** であるという．例えば，実数体 $\boldsymbol{R}$ の絶対値は，付値となるが，非アルキメデス的にはならない．

$\varphi: K\longrightarrow \boldsymbol{R}$ を非アルキメデス的付値とする．このとき

$$\mathfrak{o}=\{a\in K\mid\varphi(a)\leqq 1\},$$

$$\mathfrak{p}=\{a\in K\mid\varphi(a)<1\}$$

とおくと，(**MV 1**), (**MV 2′**) より，$\mathfrak{o}$ は K の部分環となり，$\mathfrak{p}$ は $\mathfrak{o}$ のイデアルとなる．さらに次のことがわかる．

命題 4.12 $\mathfrak{o}, \mathfrak{p}$ を上の通りとする．このとき

(1) a を任意の K の元とするとき，a または a^{-1} が $\mathfrak{o}$ に属す．

(2) $a \in \mathfrak{o}$ が単数 $\iff$ $\varphi(a) = 1$.

(3) $\mathfrak{o}$ は局所環で，$\mathfrak{p}$ は $\mathfrak{o}$ の極大イデアルである．

[**証明**] (1), (2) は $\mathfrak{o}$ の定義より明らかである．$\mathfrak{p}$ は $\mathfrak{o}$ のイデアルであり，(2) より $\mathfrak{p} = \mathfrak{o} \setminus U(\mathfrak{o})$ だから，$\mathfrak{o}$ は局所環で $\mathfrak{p}$ はその極大イデアルとなる． (証明終)

一般に，体 K の部分環 $\mathfrak{o}$ が命題 4.12 の (1) を満たすなら，$\mathfrak{o}$ を **付値環** という．このとき，$\mathfrak{o}$ は局所環で，

$$\mathfrak{p} = \{a \in \mathfrak{o} \mid a = 0 \text{ または } a^{-1} \notin \mathfrak{o}\}$$

はその極大イデアルとなる．

$\varphi : K \longrightarrow \boldsymbol{R}$ を非アルキメデス的付値とする．(**MV 1**) より，φ は K の乗法群 $K^* = K \setminus \{0\}$ より，$\boldsymbol{R}$ の乗法群 $\boldsymbol{R}^* = \boldsymbol{R} \setminus \{0\}$ への，群の準同型をひきおこす．よって $\varphi(K^*)$ は $\boldsymbol{R}^*$ の部分群となるが，これが巡回群 $\boldsymbol{Z}$ と同型となるとき，φ を **離散的付値** とよび，$\mathfrak{o} = \{a \in K \mid \varphi(a) \leqq 1\}$ を **離散的付値環** とよぶ．このとき次が成り立つ．

命題 4.13 $\varphi : K \longrightarrow \boldsymbol{R}$ を離散的付値とし，$\mathfrak{o}$ をその付値環，$\mathfrak{p}$ を $\mathfrak{o}$ の極大イデアルとする．このとき，

(1) $\mathfrak{p}$ は単項イデアルである．

(2) $\mathfrak{p} = (t)$ とすると，任意の $a \in K$ は，$a = ut^n$ (u は $\mathfrak{o}$ の単数，$n \in \boldsymbol{Z}$) と一意的に書ける．とくに $\mathfrak{o}$ は一意分解環となり，$\mathfrak{o}$ の素元は同伴の差を除き t に限る．

(3) $\mathfrak{o}$ の任意のイデアルは $\mathfrak{p}^n$ ($n \in \boldsymbol{Z}, \geqq 0$) の形である．

[**証明**] (1) $\varphi(K^*) \simeq \boldsymbol{Z}$ だから，その生成元で 1 より小なるものを $\varphi(t)$ ($t \in K$) とすると，$t \in \mathfrak{p}$ となる．しかも，b を $\mathfrak{p}$ の任意の元とすると，

$$\varphi(b) \leqq \varphi(t) \iff \varphi(bt^{-1}) \leqq 1 \iff bt^{-1} \in \mathfrak{o} \iff b \in (t)$$

であるから，$b \in (t)$ となる．よって $\mathfrak{p} = (t)$ となる．逆に $\mathfrak{p} = (t)$ なら，$\varphi(t)$ は $\varphi(K^*)$ を生成することもわかる．

（2）（1）の t は，$\mathfrak{p} = (t)$ が素イデアルだから，$\mathfrak{o}$ の素元である．a を K の 0 でない元とすると，$\varphi(t)$ は $\varphi(K^*)$ を生成するから，$\varphi(a) = \varphi(t)^n$ $(n \in \boldsymbol{Z})$ と書ける．このとき $u = at^{-n}$ は，$\varphi(u) = \varphi(a)\varphi(t)^{-n} = 1$ を満たすから，$\mathfrak{o}$ の単数となる．よって $a = ut^n$ と命題の形に書ける．表現の一意性は，$\varphi(a) = \varphi(t)^n$ より a が定まると n が定まるから，明らかである．よって（2）が成り立つ．

（3）$\mathfrak{a}$ を $\mathfrak{o}$ の $\{0\}$ でも $\mathfrak{o}$ でもないイデアルとする．このとき，$\{\varphi(a) \mid a \in \mathfrak{a}\} \subset \{\varphi(t)^n \mid 0 \leqq n \in \boldsymbol{Z}\}$ において，$\varphi(a)$ が最大となる $\varphi(a)$ $(a \in \mathfrak{a})$ をとり，$\varphi(a) = \varphi(t)^n$ とおく．そこで $\mathfrak{a}$ の任意の元 b をとると，$\varphi(b) \leqq \varphi(a)$ だから，$b = ca$ $(c \in \mathfrak{o})$ と書ける．しかも，$a = ut^n$（u は $\mathfrak{o}$ の単数）となるから，$\mathfrak{a} = (a) = (t^n) = \mathfrak{p}^n$ となる．

（証明終）

例 4．14　R を一意分解環，K を商体，P を R の素元の同値類の完全代表系とする．K の任意の元は

$$a = u \prod_{p \in P} p^{e_p(a)} \qquad (u \in U(R),\ e_p(a) \in \boldsymbol{Z},\ \text{有限個以外 } e_p(a) \text{ は } 0)$$

という形に一意的に書ける．q を P の元とするとき，

$$\varphi_q(a) = 2^{-e_q(a)}$$

とおき，$\varphi_q : K \longrightarrow \boldsymbol{R}$ を定めると，φ_q は K の離散的付値となる．φ_q の付値環は

$$R_{(q)} = \{a = u \prod_{p \in P} p^{e_p(a)} \in K \mid u \in U(R),\ e_q(a) \geqq 0,\ e_p(a) \in \boldsymbol{Z}\}$$

となる．よって $R_{(q)}$ は R の (q) における局所化であり，

$$R = \bigcap_{q \in P} R_{(q)}$$

が成り立つ．

§5. ネ タ ー 環

R を環とし，M を左 R-加群とする．このとき第 II 章，§7 の意味で，M は作用域 R をもつ加法群とみなせる．M の部分加群 N は，この意味で R-部分群となるとき，**R-部分加群** であるという．これは $RN \subset N$ を意味する．（第

IV章，1.1参照)．そこでMが第II章，§8の意味でネター的（またはアルティン的）であるとき，Mを**ネター的R-加群**（または**アルティン的R-加群**）であるという．したがって，第II章，命題8.1より，Mは以下の（同値な）3条件のうちのどれかを満たすときネター的となる．

(**NM 1**) MのR-部分加群のなす任意の空でない集合は，包含関係に関して極大な元を含む（極大条件）．

(**NM 2**) $$M_1 \subset M_2 \subset \cdots \subset M_n \subset \cdots$$
をMのR-部分加群の任意の無限増加列とすると，ある番号Nより$M_N = M_{N+1} = \cdots$ となる（昇鎖律）．

(**NM 3**) Mの任意のR-部分加群は，R-加群として有限生成である（基底律）．

アルティン的R-加群についても，第II章，命題8.3より，極小条件と降鎖律を使っての同様の特徴づけが得られる．

Mを左R-加群とし，M'をMのR-部分加群とする．このとき，加法群としての剰余群$M'' = M/M'$には自然に左R-加群の構造が入る．したがって第II章，命題8.2（または命題8.4）より，Mがネター的R-加群（またはアルティン的R-加群）なら，M'もM''も同様であり，逆にM'およびM''がネター的R-加群（またはアルティン的R-加群）ならMも同様となる．

Rを環とする．このときRの乗法により，R自身を左R-加群と思える．さらに，Rの部分集合$\mathfrak{a}$がR-部分加群となるのは，$\mathfrak{a}$がRの左イデアルとなることと同値である．そこで，Rが左R-加群とみてネター的（またはアルティン的）であるとき，Rを**左ネター環**（または**左アルティン環**）とよぶ．右ネター環や右アルティン環も同様にして定義される．とくにRが可換環のときは，左，右の区別する必要がないから，**ネター環**，**アルティン環**などとよぶ．可換環Rがネター環となるには，

(**NR 1**) Rの任意のイデアルの空でない集合は，包含関係に関し極大な元

を含む（極大条件）.

(**NR 2**) $$\mathfrak{a}_1 \subset \mathfrak{a}_2 \subset \cdots \subset \mathfrak{a}_n \subset \cdots$$

をRのイデアルの任意の無限増加列とすると，ある番号Nより$\mathfrak{a}_N = \mathfrak{a}_{N+1} = \cdots$が成り立つ（昇鎖律）.

(**NR 3**) Rの任意のイデアルは，有限個の元で生成される（基底律）.

のどれかが成り立つことが，必要かつ十分である．アルティン環についても，イデアルの極小条件または降鎖律を使って同様の定義ができる.

(**NR 3**) より，単項イデアル整域はネター環である．また，R'が可換環Rの剰余環$R/\mathfrak{a}$なら，準同型定理によりR'のイデアルと，Rの$\mathfrak{a}$を含むイデアルとは1対1に対応する．よって (**NR 1**)（または (**NR 2**)）より，Rがネター環なら，その剰余環（準同型像）R'もネター環となる.

次のヒルベルトの基底定理は，非常に重要である.

定理 5.1（ヒルベルト） 可換環Rがネター環となるなら，多項式環$R[x_1, x_2, \cdots, x_n]$もネター環となる.

［**証明**］ 帰納法により，$n=1$で，$x_1 = x$のとき証明すれば十分である.

$\mathfrak{a}$を$R[x]$のイデアルとし，$\mathfrak{a}$が有限生成であることを示す．負でない整数mに対し，

$$\mathfrak{a}_m = \{a_m \in R \mid \exists f(x) = a_0 + a_1 x + \cdots + a_m x^m \in \mathfrak{a}\}$$

とおく．$\mathfrak{a}$は$R[x]$のイデアルだから，$\mathfrak{a}_m$はRのイデアルとなる．また $f(x) = a_0 + a_1 x + \cdots + a_m x^m \in \mathfrak{a}$ なら，$xf(x) = a_0 x + a_1 x^2 + \cdots + a_m x^{m+1} \in \mathfrak{a}$ となるから，

$$\mathfrak{a}_0 \subset \mathfrak{a}_1 \subset \cdots \subset \mathfrak{a}_m \subset \cdots$$

となる．ところがRはネター環だから，(**NR 2**) により，あるNに対して$\mathfrak{a}_N = \mathfrak{a}_{N+1} = \cdots$となる．そこで$0 \leqq m \leqq N$なる$m$に対し，(**NR 3**) より$\mathfrak{a}_m = (a_{m1}, a_{m2}, \cdots, a_{m\,i(m)})$とおき，$a_{mj} \in \mathfrak{a}_m$を最高次の係数とする$\mathfrak{a}$に入る$m$次多項式を$f_{mj}(x)$ $(1 \leqq j \leqq i(m))$とおく．このとき，$\mathfrak{a}$が$f_{mj}(x)$ $(0 \leqq m \leqq N,\ 1 \leqq j \leqq i(m))$により生成されることを以下で示す.

実際，$f(x) = a_0 + a_1 x + \cdots + a_l x^l \in \mathfrak{a}$ とすると，$a_l \in \mathfrak{a}_l$となる．もし$l > N$なら，$\mathfrak{a}_N = \mathfrak{a}_{N+1} = \cdots = \mathfrak{a}_l$であるから，$f(x) - x^{l-N}\,(b_1 f_{N1}(x) + b_2 f_{N2}(x) + \cdots + b_{i(N)} f_{N i(N)}(x)) \in \mathfrak{a}$ $(\exists b_1, b_2, \cdots, b_{i(N)} \in R)$は高々$l-1$次の多項式となる．もし$l \leqq$

N なら，$f(x)-\sum b_j f_{ij}(x)\in\mathfrak{a}$ が高々 $l-1$ 次の多項式となる．したがって，$\deg f(x)$ に関する帰納法により，

$$f(x)=\sum g_{mj}(x)f_{mj}(x) \qquad (g_{mj}(x)\in R[x],\ 0\leqq m\leqq N,\ 1\leqq j\leqq i(m))$$

と書けることがわかる．したがって，$\mathfrak{a}$ は有限生成なイデアルとなり，$R[x]$ はネター環となる．（証明終）

例 5.2 S を可換環とし，R を S の部分環で，S の任意の元が，$a_1, a_2, \cdots, a_n\in S$ についての R 係数の多項式で表されるとする．このとき，S は **環 R 上 $a_1, a_2, \cdots, a_n$ により生成される** という．そこで，写像 $f: R[x_1, x_2, \cdots, x_n]\longrightarrow S$ を，

$$\sum c_{i_1 i_2\cdots i_n}x_1{}^{i_1}x_2{}^{i_2}\cdots x_n{}^{i_n} \longmapsto \sum c_{i_1 i_2\cdots i_n}a_1{}^{i_1}a_2{}^{i_2}\cdots a_n{}^{i_n}$$

で定義すると，これは S の上への環の準同型となる．したがって，S は多項式環 $R[x_1, x_2, \cdots, x_n]$ の剰余環と同型となる．

そこで，S が可換環で，その部分環 R 上有限個の元で生成され，しかも R がネター環であるとする．このとき，定理 5.1 より，R 上の多項式環はネター環である．したがって，R 上の多項式環の剰余環と同型な S も，ネター環となる．

問題 5.3 R をネター環とする．このとき，形式的べき級数環 $R[[x_1, x_2, \cdots, x_n]]$ もネター環となることを示せ．

（ヒント）．$n=1$ とし，$\mathfrak{a}$ を $R[[x]]$ のイデアルとする．このとき，

$$\mathfrak{a}_m=\{a_m\in R \mid \exists f(x)=a_m x^m+a_{m+1}x^{m+1}+a_{m+2}x^{m+2}+\cdots\in\mathfrak{a}\}$$

を考えよ．

問題 5.4 R を可換環，S を R の乗法的閉集合，$i: R\longrightarrow R_S$ を商環への自然な写像とする．このとき $\mathfrak{a}$ を R_S のイデアルとすると，$i^{-1}(\mathfrak{a})$ は R のイデアルで，$i(i^{-1}(\mathfrak{a}))$ はイデアル $\mathfrak{a}$ を生成することを示せ．さらにこれより，R がネター環なら，その商環 R_S もネター環となることを示せ．

§6. ネター環におけるイデアル論

6.1 準素イデアルと根基 R を可換環，$\mathfrak{a}$ を R のイデアルとするとき，

$$\sqrt{\mathfrak{a}}=\{a\in R \mid a \text{ の適当なべき } a^e \text{ が } \mathfrak{a} \text{ に属す}\}$$

を$\mathfrak{a}$の**根基**という．$a, a_1, a_2 \in \sqrt{\mathfrak{a}}$とし，$a^e, a_1^{e_1}, a_2^{e_2} \in \mathfrak{a}$，$r \in R$とすると，

$$(ra)^e = r^e a^e \in \mathfrak{a}, \qquad (a_1 + a_2)^{e_1+e_2} = \sum_{0 \leqq i \leqq e_1+e_2} \binom{e_1 + e_2}{i} a_1{}^i a_2{}^{e_1+e_2-i} \in \mathfrak{a}$$

となるから，$\sqrt{\mathfrak{a}}$もRのイデアルとなる．とくに，$\sqrt{\{0\}} = \{a \in R \mid a^e = 0$ $(\exists e \geqq 1)\}$ をRの**べき零根基**といい，その元を**べき零元**という．

定理 6.1　$\sqrt{\mathfrak{a}}$は$\mathfrak{a}$を含む素イデアル全体の共通部分に等しい．

［**証明**］ $\pi : R \longrightarrow R/\mathfrak{a}$を自然な準同型とすると，準同型定理により，$R$の$\mathfrak{a}$を含む素イデアルと$R/\mathfrak{a}$の素イデアルが1対1に対応する．また，$R$の根基$\sqrt{\mathfrak{a}}$は，$R/\mathfrak{a}$のべき零根基に対応する．よって，$\mathfrak{a} = \{0\}$とし，$R$のべき零根基が$R$の素イデアル全体の共通部分となることを示せば十分である．

$\mathfrak{p}$をRの素イデアルとし，$a \in \sqrt{\{0\}}$とする．このとき適当なeに対し，$a^e = 0$となる．よって$a \cdot a \cdots a = a^e = 0 \in \mathfrak{p}$となるから，$a \in \mathfrak{p}$となる．したがって$\sqrt{\{0\}} \subset \mathfrak{p}$となる．

次に $a \notin \sqrt{\{0\}}$ とする．このとき $S = \{a^n \mid n = 0, 1, 2, \cdots\}$ はRの乗法的閉集合となる．そこで $i : R \longrightarrow R' = R_S$ を商環とし，R'の極大イデアル$\mathfrak{p}'$をとり，$\mathfrak{p} = i^{-1}(\mathfrak{p}')$ とおく．準同型定理より，$\mathfrak{p}$はRのイデアルで，$R/\mathfrak{p} \hookrightarrow R'/\mathfrak{p}'$となる．$R'/\mathfrak{p}'$は体だから，$R/\mathfrak{p}$は整域となり，$\mathfrak{p}$は$R$の素イデアルとなる．また$S$の元には$R'$の単数が対応するから，極大イデアル$\mathfrak{p}'$の元は対応せず，$S \cap \mathfrak{p} = \emptyset$となる．とくに$a \notin \mathfrak{p}$となるから，対偶をとり，$\sqrt{\{0\}} \supset \cap\, \mathfrak{p}$（$\mathfrak{p}$は素イデアルを動く）を得る．（証明終）

Rのイデアル$\mathfrak{q}$で，条件

(PR)　　$ab \in \mathfrak{q},\ a \notin \mathfrak{q} \Longrightarrow$ あるbのべき $b^e \in \mathfrak{q}$

を満たすものを**準素イデアル**という．素イデアルは準素イデアルであるが，逆は一般には成り立たない．

命題 6.2　$\mathfrak{q}$を可換環Rの準素イデアルとする．このとき，$\mathfrak{p} = \sqrt{\mathfrak{q}}$は$\mathfrak{q}$を含む最小の素イデアルとなる．以下，$\mathfrak{p}$と$\mathfrak{q}$がこのような関係にあるとき，$\mathfrak{q}$は素イデアル$\mathfrak{p}$**に属する準素イデアル**であるという．

［**証明**］ 最小性は定理6.1より明らかである．$\mathfrak{q}$は準素イデアルだから，$R/\mathfrak{q}$において

$$\bar{a}\bar{b} = 0,\ \bar{a} \neq 0 \implies \bar{b}^e = 0 \quad (\exists e \geqq 1)$$

が成り立つ．この様な元 $\bar{b}$ は $R/\mathfrak{q}$ のべき零根基 $\sqrt{\{0\}} = \bar{\mathfrak{p}}$ に含まれるから，

$$ab \in \mathfrak{p},\ a \notin \mathfrak{p} \implies (ab)^f \in \mathfrak{q},\ a \notin \mathfrak{q}\ (\exists f \geqq 1) \implies b \in \mathfrak{p}$$

が成り立つ．よって $\mathfrak{p}$ は素イデアルである． (証明終)

例 6.3 k を体，$R = k[x]$ とする．このとき，$\mathfrak{q} = (x^2)$ は準素イデアルで，$\sqrt{\mathfrak{q}} = (x)$ となる．

6.2 準素イデアル分解

以下 6.2 では，次の定理を証明する．

定理 6.4 ネター環 R の任意のイデアル $\mathfrak{a}$ は，有限個の準素イデアルの交わり $\mathfrak{q}_1 \cap \mathfrak{q}_2 \cap \cdots \cap \mathfrak{q}_n$ の形に表される．しかも，この様な表示でむだのないものをとれば，対応する素イデアルの集合 $\{\sqrt{\mathfrak{q}_1}, \sqrt{\mathfrak{q}_2}, \cdots, \sqrt{\mathfrak{q}_n}\}$ は，$\mathfrak{a}$ により一意的に定まる．ここで**むだがない**とは，$\mathfrak{a}$ が $\{\mathfrak{q}_1, \mathfrak{q}_2, \cdots, \mathfrak{q}_n\}$ の真部分集合の交わりには表されぬことをいう．

R を可換環とし，$\mathfrak{a} \subsetneqq R$ をイデアルとする．このとき，$\mathfrak{b} \supsetneqq \mathfrak{a}$, $\mathfrak{c} \supsetneqq \mathfrak{a}$ なるイデアル $\mathfrak{b}, \mathfrak{c}$ で $\mathfrak{a} = \mathfrak{b} \cap \mathfrak{c}$ なるものが存在しないとき，$\mathfrak{a}$ を**既約**であるという．

R を可換環とし，$\mathfrak{a}, \mathfrak{b}$ を R のイデアルとする．このとき

$$\mathfrak{a} : \mathfrak{b} = \{c \in R \mid c\mathfrak{b} \subset \mathfrak{a}\}$$

とおく．これは，R の $\mathfrak{a}$ を含むイデアルとなる．これを，$\mathfrak{a}$ の $\mathfrak{b}$ による**イデアル商**という．

命題 6.5 ネター環の既約イデアルは準素イデアルである．

[証明] $\mathfrak{a}$ をネター環 R の準素でないイデアルとし，$\mathfrak{a}$ が既約でないことを示す．よって，$a, b \in R$ で，

$$ab \in \mathfrak{a}, \qquad a \notin \mathfrak{a}, \qquad b^e \notin \mathfrak{a} \quad (\forall e = 1, 2, 3, \cdots)$$

なるものが存在するとする．R はネター環だから，

$$\mathfrak{a} = \mathfrak{a} : (1) \subset \mathfrak{a} : (b) \subset \mathfrak{a} : (b^2) \subset \cdots$$

なる列は，ある番号 N より $\mathfrak{a} : (b^N) = \mathfrak{a} : (b^{N+1}) = \mathfrak{a} : (b^{N+2}) = \cdots$ を満たす．そこで $\mathfrak{b} = \mathfrak{a} : (b^N)$, $\mathfrak{c} = (\mathfrak{a}, b^N)$ とおくと，$\mathfrak{b} \ni a$, $\mathfrak{c} \ni b^N$ だから，$\mathfrak{b} \supsetneqq \mathfrak{a}$, $\mathfrak{c} \supsetneqq \mathfrak{a}$ となる．

そこで$t \in \mathfrak{b} \cap \mathfrak{c}$を任意にとる．$t$は$\mathfrak{c}$の元だから，$t = a_1 + rb^N$ ($a_1 \in \mathfrak{a}$, $r \in R$) と書ける．このとき，tは$\mathfrak{b}$にも属するから，$tb^N \in \mathfrak{a}$となる．よって $tb^N = a_1b^N + rb^{2N} \in \mathfrak{a}$, $a_1 \in \mathfrak{a}$だから，$rb^{2N} \in \mathfrak{a}$となる．したがって，$r \in \mathfrak{a} : (b^{2N}) = \mathfrak{a} : (b^N)$ となるから，$t = a_1 + rb^N \in \mathfrak{a}$となる．したがって，$\mathfrak{b} \cap \mathfrak{c} \subset \mathfrak{a}$が成り立つから，$\mathfrak{a} = \mathfrak{b} \cap \mathfrak{c}$となり，$\mathfrak{a}$は既約ではない． (証明終)

定理6.4の表示の存在は，命題6.5と次の補題よりわかる．

補題6.6 ネター環のイデアルは，有限個の既約イデアルの交わりとして表される．

[証明] ネター環Rにおいて，補題が成り立たないものとする．そこで，Rのイデアルで，このような形に書けないものの全体を$\mathscr{B}$とおく．$\mathscr{B}$に包含関係で順序を入れる．$\mathscr{L} = \{\mathfrak{a}_\lambda \mid \lambda \in \Lambda\}$ を$\mathscr{B}$の全順序部分集合とする．Rはネター環で，$\mathfrak{a}_\lambda$はRのイデアルだから，$\mathscr{L} = \{\mathfrak{a}_\lambda\}$ には最大元が存在する．よって$\mathscr{B}$は帰納的順序集合となり，極大元$\mathfrak{a} \in \mathscr{B}$が存在する．このとき$\mathscr{B}$の定め方より，$\mathfrak{a} = \mathfrak{b} \cap \mathfrak{c}$, $\mathfrak{b} \supsetneqq \mathfrak{a}$, $\mathfrak{c} \supsetneqq \mathfrak{a}$の形に表される．$\mathfrak{a}$は$\mathscr{B}$の極大元だから，$\mathfrak{b} \notin \mathscr{B}$, $\mathfrak{c} \notin \mathscr{B}$である．よって$\mathfrak{b}, \mathfrak{c}$は有限個の既約イデアルの交わりと書け，$\mathfrak{a} = \mathfrak{b} \cap \mathfrak{c}$も有限個の既約イデアルの交わりとなる．これは$\mathfrak{a} \in \mathscr{B}$に矛盾する． (証明終)

定理6.4の一意性は，次の補題の (2) が，$\mathfrak{a}$の表示によらないことからでる．

補題6.7 $\mathfrak{a}$をネター環Rのイデアル，$\mathfrak{a} = \mathfrak{q}_1 \cap \mathfrak{q}_2 \cap \cdots \cap \mathfrak{q}_n$を$\mathfrak{a}$の準素イデアルによるむだのない表示，$\mathfrak{p}$を$R$の素イデアルとする．このとき次は同値である．

(1) $\mathfrak{p}$はある準素イデアル $\mathfrak{q}_i$ $(1 \leqq i \leqq n)$ の根基$\sqrt{\mathfrak{q}_i}$と一致する．

(2) $\mathfrak{a}$に属さない元cで，$\mathfrak{a} : (c)$ が$\mathfrak{p}$に属する準素イデアルとなるものが存在する．

[証明] (1)$\Longrightarrow$(2)． $\mathfrak{a} = \mathfrak{q}_1 \cap \mathfrak{q}_2 \cap \cdots \cap \mathfrak{q}_n$を補題のものとし，$\mathfrak{p} = \sqrt{\mathfrak{q}_i}$であるとする．これはむだのない表示だから，$\mathfrak{q}_i$には属さず，他のすべての$\mathfrak{q}_j$ $(j \neq i)$ に属する元cが存在する．$c \notin \mathfrak{q}_i$だから$c \notin \mathfrak{a}$である．また $(c)\mathfrak{q}_i \subset (\bigcap_{j \neq i} \mathfrak{q}_j) \cap \mathfrak{q}_i = \mathfrak{a}$だから，

$\mathfrak{q}_i \subset \mathfrak{a} : (c)$ となる．そこで $t \in \mathfrak{a} : (c)$ とすると，$tc \in \mathfrak{a} \subset \mathfrak{q}_i$，$c \notin \mathfrak{q}_i$ より $t \in \sqrt{\mathfrak{q}_i}$ となる．よって $\mathfrak{a} : (c) \subset \mathfrak{p}$ が成り立つ．

$xy \in \mathfrak{a} : (c)$，$x^e \notin \mathfrak{a} : (c)$ $(e = 1, 2, \cdots)$ とする．$x^e \notin \mathfrak{q}_i \subset \mathfrak{a} : (c)$ だから，$x \notin \sqrt{\mathfrak{q}_i} = \mathfrak{p}$ である．よって $xyc \in \mathfrak{a} \subset \mathfrak{q}_i$ より，$yc \in \mathfrak{q}_i$ となる．他方 $c \in \mathfrak{q}_j$ だから，$yc \in (\bigcap_{j \neq i} \mathfrak{q}_j) \cap \mathfrak{q}_i = \mathfrak{a}$ となる．よって $y \in \mathfrak{a} : (c)$ となる．$xy \in \mathfrak{a} : (c)$，$x^e \notin \mathfrak{a} : (c)$ $(e = 1, 2, \cdots)$ より $y \in \mathfrak{a} : (c)$ が導けたから，$\mathfrak{a} : (c)$ は準素イデアルである．しかも $\mathfrak{q}_i \subset \mathfrak{a} : (c) \subset \mathfrak{p} = \sqrt{\mathfrak{q}_i}$ だから，$\mathfrak{a} : (c)$ も $\mathfrak{p}$ に属する準素イデアルとなる．

（2）$\Longrightarrow$（1）． c を（2）のようにとる．$\mathfrak{a} = \mathfrak{q}_1 \cap \mathfrak{q}_2 \cap \cdots \cap \mathfrak{q}_n$ だから，$\mathfrak{a} : (c) = (\bigcap_i \mathfrak{q}_i) : (c) = \bigcap_i (\mathfrak{q}_i : (c))$ である．したがって，$\mathfrak{p} = \sqrt{\mathfrak{a} : (c)} = \bigcap_i \sqrt{\mathfrak{q}_i : (c)}$ で，$\mathfrak{p}$ は素イデアルだから，ある i について $\mathfrak{p} = \sqrt{\mathfrak{q}_i : (c)}$ となる．ここで $c \in \mathfrak{q}_i$ とすれば $\mathfrak{q}_i : (c) = R$ となり矛盾するから，$c \notin \mathfrak{q}_i$ である．ところが $\mathfrak{q}_i$ は準素イデアルだから，$\mathfrak{q}_i : (c) \subset \sqrt{\mathfrak{q}_i}$ となる．よって $\mathfrak{p} = \sqrt{\mathfrak{q}_i : (c)} = \sqrt{\mathfrak{q}_i}$ となる． （証明終）

例 6.8 k を体，$R = k[x, y]$，$\mathfrak{a} = (x^2, xy)$ とおく．$\mathfrak{q}_1 = (x)$，$\mathfrak{q}_2 = (x^2, xy, y^2)$，$\mathfrak{q}_3 = (x^2, y)$ とおくと，$\sqrt{\mathfrak{q}_1} = \mathfrak{q}_1 = (x)$，$\sqrt{\mathfrak{q}_2} = (x, y)$，$\sqrt{\mathfrak{q}_3} = (x, y)$ であり，$\mathfrak{a} = \mathfrak{q}_1 \cap \mathfrak{q}_2 = \mathfrak{q}_1 \cap \mathfrak{q}_3$ は共に準素イデアルによるむだのない表示となる．この場合 $\{\mathfrak{q}_1, \mathfrak{q}_2\} \neq \{\mathfrak{q}_1, \mathfrak{q}_3\}$ だが，$\{\sqrt{\mathfrak{q}_1}, \sqrt{\mathfrak{q}_2}\} = \{\sqrt{\mathfrak{q}_1}, \sqrt{\mathfrak{q}_3}\}$ が成り立つ．

6.3 デデキンド環* S を可換環とし，R をその部分環とする．S の元 x が

$$x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 = 0 \qquad (a_i \in R)$$

の形の方程式を満たすなら，**x は R 上整** であるという．

$x \in S$ が部分環 R 上整となるための必要十分条件は，$R[x] \subset S$ が有限生成 R–加群となることである．これを使うと，S の元で R 上整なもの全体は S の部分環をなすことがわかる．これを R の S の中での **整閉包** とよぶ．

S の任意の元が R 上整のとき，**S は R 上整** であるという．また，S の元で R 上整なものが R の元に限るなら，**R は S の中で整閉** であるという．とくに，R が整閉で S が R の商体のとき，R が商体 S の中で整閉なら，**R は整閉** であるという．

一意分解環は，この意味で整閉なことは容易にわかる．また，R の S の中での整閉包を S_0 とすると，S_0 は S の中で整閉なこともわかる．

$S \supset R$ を整域とし，S が R 上整であるとする．このとき，S が体となるための必要十分条件は，R が体となることである．これを剰余環に対して使うと，整域 S が R 上整で，S の素イデアル $\mathfrak{q}$ の R への制限を $\mathfrak{p}=\mathfrak{q}\cap R$ とするとき，$\mathfrak{q}$ が S の極大イデアルとなるための必要十分条件は，$\mathfrak{p}$ が R の極大イデアルであることがわかる．

R を整域，K を R の商体，L を K を含む体とし，S を L の中での R の整閉包とする．このとき S は整閉であり，また R の $\{0\}$ 以外の素イデアルが極大イデアルに限るなら，S においても同様となる．R がネター環であっても，S はネター環となるとは限らないが，L が K の有限次分離拡大(第V章，§1，§4 参照）なら，S もネター環となることが証明できる．

整域 R は，次の条件を満たすとき，**デデキンド環** であるという：

(D 1)　R はネター的である．

(D 2)　R の $\{0\}$ 以外の素イデアルは極大イデアルである．

(D 3)　R は整閉である．

例 6. 9　有理数体 $\boldsymbol{Q}$ の有限次拡大を（有限次）**代数体** という．L を代数体とし，$\mathfrak{o}$ を L の中での整数のなす環 $\boldsymbol{Z}$ の整閉包とする．$\boldsymbol{Z}$ は単項イデアル整域だから，**(D 1)** ～ **(D 3)** が成り立ちデデキンド環となる．ところが，$L/\boldsymbol{Q}$ は分離的だから，$\mathfrak{o}$ についても **(D 1)** ～ **(D 3)** が成り立ち，$\mathfrak{o}$ もデデキンド環となる．$\mathfrak{o}$ を代数体 L の **整数環** とよぶ．

デデキンド環において，準素イデアル分解（定理 6.4）は次の形となる．

定理 6. 10　R を整域とする．このとき，

（1）　R が **(D 1)**, **(D 2)** を満たすなら，任意の $\{0\}$ でない R のイデアル $\mathfrak{a}$ は，準素イデアルの積 $\mathfrak{a}=\mathfrak{q}_1\mathfrak{q}_2\cdots\mathfrak{q}_n$，$\sqrt{\mathfrak{q}_i}\neq\sqrt{\mathfrak{q}_j}$ $(i\neq j)$ の形に一意的に書ける．

（2）　R が **(D 1)** ～ **(D 3)** を満たしデデキンド環となるなら，R の準素イ

デアルは，素イデアルのべきの形に書ける．したがって，デデキンド環においては，任意の $\{0\}$ でないイデアル $\mathfrak{a}$ は，素イデアルのべき積 $\mathfrak{a}=\mathfrak{p}_1^{e_1}\mathfrak{p}_2^{e_2}\cdots\mathfrak{p}_n^{e_n}$ ($\mathfrak{p}_i$ は相異なる素イデアル，$e_i \geqq 1$) の形に一意的に表される．

（3） 逆に，整域 R において，任意の $\{0\}$ 以外のイデアルが素イデアルのべき積の形に一意的に表されるなら，R はデデキンド環となる．

（注） 定理 6.4 および定理 6.10 は，ネター環において，素元分解の一意性（4.1 参照）が，どのような形で拡張されるかをのべている．定理 6.10 の証明は，かなり面倒であるので省略する．

例 6. 11 $L=\boldsymbol{Q}(\sqrt{-5})=\{a+b\sqrt{-5}\mid a,b\in\boldsymbol{Q}\}$ とおく．このとき，L は代数体で，その整数環は $\mathfrak{o}=\boldsymbol{Z}+\boldsymbol{Z}\sqrt{-5}=\{a+b\sqrt{-5}\mid a,b\in\boldsymbol{Z}\}$ となる．$\mathfrak{o}$ において

$$6=2\cdot 3=(1+\sqrt{-5})(1-\sqrt{-5})$$

という 2 通りの素元分解がある．しかし，イデアルとしては，

$$(2)=(2,1+\sqrt{-5})^2,\qquad (3)=(3,1+\sqrt{-5})(3,1-\sqrt{-5}),$$
$$(1\pm\sqrt{-5})=(2,1+\sqrt{-5})(3,1\pm\sqrt{-5})$$

とさらに分解される．したがって，

$$(6)=(2,1+\sqrt{-5})^2(3,1+\sqrt{-5})(3,1-\sqrt{-5})$$

と，素イデアルのべき積としては一意的に表される．

問　　　題

1. 斜体 D の真の部分斜体 C で，任意の $a\in D, a\neq 0$ に対し $a^{-1}Ca=C$ を満たすものは，D の中心に含まれることを示せ（カルタン・ブラウアーの定理）．

（ヒント） $c\in C, a\in D, a\neq 0, -1$ に対し，$c_1=a^{-1}ca$,　$c_2=(1+a)^{-1}c(1+a)$ とおくと，$a(c_2-c_1)=c-c_2$ が成り立つ．

2. 有理数体 $\boldsymbol{Q}$ の部分環は，整数環 $\boldsymbol{Z}$ の適当な乗法的閉集合 S をとると，$\boldsymbol{Z}_S$ の形となることを示せ．

3. R を一意分解環とし，p を R の素元とする．原始的多項式 $f(x)=a_0+a_1x+\cdots+a_{n-1}x^{n-1}+a_nx^n\in R[x]$ が条件

$$p \mid a_i \quad (i = 0, 1, \cdots, n-1), \quad p^2 \nmid a_0, \quad p \nmid a_n$$

を満たすなら，$f(x)$ は既約であることを示せ（アイゼンシュタインの判定法）.

4. （1） 次の多項式 $i(x), h(x) \in \boldsymbol{Z}[x]$ の既約性を判定せよ.

$$i(x) = x^3 + 2x + 5, \qquad h(x) = x^4 + 3x + 1.$$

（2） $\boldsymbol{Z}$ においては，ユークリッドの互除法により，有限回の操作で素因数分解ができる．第 I 章末の問題 2 を使い，任意の整数係数の多項式 $f(x) \in \boldsymbol{Z}[x]$ を，有限回の操作で素因数分解する方法を作れ.

（ヒント） $f(x)$ の因子 $g(x)$ は，$g(m) \mid f(m)$ $(m = 0, 1, \cdots, \deg f(x))$ を満たす.

5. $R = \boldsymbol{C}[x, y, z]/(x^2 - yz)$ なる環では，$x^2 = yz$ は 2 通りの素元分解を与えることを示せ.

6. R をネター環，$\mathfrak{a}, \mathfrak{b}$ を R のイデアルとする.

（1） $R[x]$ の部分環

$$S = \{f(x) = \sum_{i=0}^{\infty} a_i x^i \in R[x] \mid a_i \in \mathfrak{a}^i\}$$

はネター環となることを示せ.

（2） S のイデアル $S \cap \mathfrak{b}[x]$ の基底を $f_1, f_2, \cdots, f_s$ ととると，$b \in \mathfrak{a}^i \cap \mathfrak{b}$ $(i \geqq k = \max \deg f_j)$ は，

$$bx^i = g_1 f_1 + g_2 f_2 + \cdots + g_s f_s \qquad (g_j \in S)$$

と書ける．この式の x^i の係数を比較することにより，

$$\mathfrak{a}^i \cap \mathfrak{b} = \mathfrak{a}^{i-k}(\mathfrak{a}^k \cap \mathfrak{b}) \qquad (\forall\, i \geqq k)$$

が成り立つことを示せ（アルティン・リースの定理）.

7. R を可換環とするとき，次のことを示せ.

（1） $\mathfrak{a}, \mathfrak{b}$ を R のイデアルで，$\mathfrak{b}$ は有限生成だとする．このとき，$\mathfrak{a}\mathfrak{b} = \mathfrak{b}$ なら，$a \in \mathfrak{a}$ で $(1-a)\mathfrak{b} = 0$ となるものが存在する.

（2） R をネター環とし，$\mathfrak{a}$ を R のイデアルとする．このとき，$\mathfrak{a}^* = \bigcap_{i=1}^{\infty} \mathfrak{a}^i$ は $\mathfrak{a}^* = \mathfrak{a} \cdot \mathfrak{a}^*$ を満たすことを示せ．さらに，

$$\mathfrak{a}^* = \{x \in R \mid \exists\, a \in \mathfrak{a}, \ ax = x\}$$

となることを示せ.

（3） ネター的局所環の極大イデアル $\mathfrak{m}$ は，$\bigcap_{i=1}^{\infty} \mathfrak{m}^i = \{0\}$ を満たすことを示せ.

8. 多項式環 $\boldsymbol{C}[x, y]$ の部分環 $R = \boldsymbol{C} + x\boldsymbol{C}[x, y]$ は，部分環 $\boldsymbol{C}$ 上有限生成とはならないことを示せ.

（ヒント） $R \cap x\boldsymbol{C}[y]$ は $\boldsymbol{C}$ 上無限次元のベクトル空間であり，$\boldsymbol{C}xg_1 + \boldsymbol{C}xg_2 + \cdots + \boldsymbol{C}xg_m$ $(g_1, g_2, \cdots, g_m \in \boldsymbol{C}[x, y])$ の形には書けない.

9. デデキンド環のイデアルは，2元で生成されることを示せ.

（ヒント） $\mathfrak{a}$ をデデキンド環 R のイデアルとする．$\mathfrak{a}$ の任意の元 $a \neq 0$ をとり，$\mathfrak{a} = \mathfrak{p}_1^{e_1}\mathfrak{p}_2^{e_2}\cdots\mathfrak{p}_t^{e_t}$，$(a) = \mathfrak{p}_1^{f_1}\mathfrak{p}_2^{f_2}\cdots\mathfrak{p}_t^{f_t}$ $(0 \leqq e_i \leqq f_i)$ と素イデアル分解をする．このとき，$b \in R$ が $\mathfrak{p}_i^{e_i}$ $(i = 1, 2, \cdots, t)$ でちょうど割り切れるなら，$\mathfrak{a} = (a, b)$ となる.

10. k を体，$R = k[x, y, z]$ とする．このとき $\mathfrak{q} = (x^2, yz + 1)$ は，素イデアル $\mathfrak{p} = (x, yz + 1)$ に属する準素イデアルであることを示せ.

（ヒント） $f(x, y, z) = \sum f_m(y, z)x^m$ と展開して考えよ.

11. $f(x), g(x) \in \boldsymbol{Z}[x]$ が，無限個の整数 $n \in \boldsymbol{Z}$ において $f(n)/g(n) \in \boldsymbol{Z}$ となるものとする．このとき，$f(x)/g(x) \in \boldsymbol{Q}[x]$ となることを示せ.

（ヒント） 一意分解環 $\boldsymbol{Z}[x]$ において，$f(x), g(x)$ が互いに素なら，$\boldsymbol{Q}[x]$ において $a^*(x)f(x) + b^*(x)g(x) = 1$ と書ける．この式の分母を払って，$a(x)f(x) + b(x)g(x) = d$ $(a(x), b(x) \in \boldsymbol{Z}[x],\ 0 \neq d \in \boldsymbol{Z})$ と書き，$d/g(x)$ を考える.

12. $\mathfrak{p}$ を多項式環 $\boldsymbol{Z}[x]$ の素イデアルで，$\{0\}$ でないものとする.

（1） $\mathfrak{p} \cap \boldsymbol{Z} = \{0\}$ なら，$\mathfrak{p}$ はある原始的既約多項式 $f(x)$ により生成されることを示せ.

（2） $\mathfrak{p} \cap \boldsymbol{Z} \neq \{0\}$ なら，$\mathfrak{p}$ はある素数 p で生成されるか，ある素数 p と，原始的既約多項式 $f(x)$ で生成されることを示せ.

13. 可換環 R において，すべてのイデアル $\mathfrak{a} \subsetneqq R$ が素イデアルなら，R は体となることを示せ.

（ヒント） R は整域である．$R \ni a \neq 0$ が逆元を持たないなら，$\mathfrak{p} = (a^2) \not\ni a$ を考え矛盾を導け.

14. $\mathfrak{p}_1, \mathfrak{p}_2, \cdots, \mathfrak{p}_t$ を可換環 R の素イデアルとするとき，$\bigcup_{i=1}^{t} \mathfrak{p}_i \subsetneqq R$ を示せ.

IV 加　群*

Rを環とし，Mをアーベル群（演算は加法 $+$ で表す）とする．このとき，R の Mへの作用 $R \times M \longrightarrow M$で，

$$r\cdot(m + m') = r\cdot m + r\cdot m', \qquad (r + r')\cdot m = r\cdot m + r'\cdot m,$$
$$(r\cdot r')\cdot m = r\cdot(r'\cdot m), \qquad\qquad 1\cdot m = m$$

$(r, r' \in R,\ m, m' \in M)$ が成り立つものを，左 R–加群とよぶ（I，§7参照）．$\{0\}$ は左 R–加群をなすが，これを 0 とも表す．この章では，主に左 R–加群の性質を調べる．

上の定義で，左，右を逆にすることにより右 R–加群も定義される．とくに R が可換環のときは，

$$m\cdot r = r\cdot m \qquad (m \in M,\ r \in R)$$

とおくことにより，左 R–加群には右 R–加群の構造が入り，その逆も成り立つ．したがって，この場合は，単に R–加群とよぶことが多い．

§1. 部分加群，剰余加群など

1.1 部分加群と剰余加群　Rを単位元 1 をもつ環とし，Mを左 R–加群とする．

NをMの部分群とするとき，

$$R\cdot N \subset N$$

が成り立つなら，NをMの **R–部分加群** であるという．このとき剰余群 M/N の上には，

$$r\cdot(m + N) = r\cdot m + N \qquad (r \in R,\ m \in M)$$

とおくことにより，左 R–加群の構造が入る．これを M の R–部分加群 N による **剰余加群** とよぶ．環の場合と同様に，剰余加群 M/N の元 $m+N$ ($m\in M$) のことを，$m \pmod N$ と表し，$m+N=m'+N$ ($m,m'\in N$) のとき $m\equiv m' \pmod N$ と表す．

M' も左 R–加群であるとする．このとき，アーベル群の準同型 $f: M\longrightarrow M'$ で，

$$f(r\cdot m)=r\cdot f(m) \qquad (r\in R,\ m\in M)$$

を満たすものを，（左 R–加群の）**準同型写像**（または **線型写像**）とよび，その全体を $\mathrm{Hom}_R(M,M')$ で表す．$\mathrm{Hom}_R(M,M')$ は

$$(f_1+f_2)(m)=f_1(m)+f_2(m) \qquad (f_1,f_2\in \mathrm{Hom}_R(M,M'),\ \ m\in M)$$

によりアーベル群をなす．さらに，M' が (R,S)–両側加群（第Ⅰ章，§7参照）なら，$\mathrm{Hom}_R(M,M')$ は

$$(f\cdot s)(m)=f(m)\cdot s \qquad (f\in \mathrm{Hom}_R(M,M'),\ \ s\in S,\ \ m\in M)$$

により右 S–加群をなす．準同型写像 $f: M\longrightarrow M'$ の **像** を $\mathrm{Im}(f)=\{f(m)\mid m\in M\}$，**核** を $\mathrm{Ker}(f)=\{m\in M\mid f(m)=0\}$ で定義する．

左 R–加群の間の準同型の列

$$\cdots\longrightarrow M_{n-1}\xrightarrow{f_{n-1}} M_n\xrightarrow{f_n} M_{n+1}\longrightarrow\cdots$$

において

$$\mathrm{Im}(f_{n-1})=\mathrm{Ker}(f_n)$$

がすべての n について成り立つとき，上の列は **完全列** であるという．とくに

$$0\longrightarrow M_1\longrightarrow M_2\longrightarrow M_3\longrightarrow 0$$

の形の完全列は，**短完全列** とよばれ，重要である（第Ⅱ章，§2参照）．

M を左 R–加群とすると，M は第Ⅱ章，§7の意味で，作用域 R をもつ群となる．また M のいまの意味での R–部分加群と，第Ⅱ章，§7の意味での R–部分群とは一致し，双方での準同型写像の定義も一致する．よって，第Ⅱ章，§7の定理7.1より，左 R–加群に対しても **準同型定理** が成り立つ．また，第Ⅱ章，8.1，8.2の結果も使える．

Mを左R–加群とする．このとき$m \in M$は，Rの零因子でない元rが$r \cdot m = 0$を満たすとき，**ねじれ元**であるという．また$m \in M$は，Rの任意の零因子でない元rに対し，$r \cdot m' = m$となる$m' \in M$が存在するとき，**可除元**であるという．さらに，Mのすべての元がねじれ元（または可除元）であるとき，Mは**ねじれ加群**（または**可除加群**）であるという．Rが可換環なら，左R–加群Mのねじれ元全体を$t(M)$とおくと，$t(M)$はR–部分加群となり，$M/t(M)$はねじれ元をもたない．

1.2　直積と直和　Rを環とし，$\{M_i\}_{i \in I}$を左R–加群の族とする（したがって，$\{M_i\}$の中に同じものがあってもよいものとする）．このとき，各$i \in I$に対して$m_i \in M_i$をとり出して並べた列の全体

$$M = \{(m_i) \mid m_i \in M_i \ \ (i \in I)\}$$

を，$\{M_i\}_{i \in I}$の直積とよぶ．Mには，

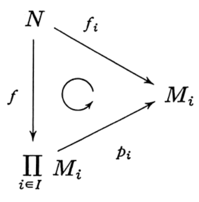
$$(m_i) + (m_i') = (m_i + m_i')$$
$$r \cdot (m_i) = (r \cdot m_i)$$

により左R–加群の構造が入る．この加群を$\prod_{i \in I} M_i$で表し，左R–加群の**直積**とよぶ．また各$i \in I$に対し，

$$p_i : \quad M \ni (m_i) \longmapsto m_i \in M_i$$

は，左R–加群の準同型写像となる．これを**標準的全射**とよぶ．

Nを左R–加群とし，各$i \in I$に対し，左R–加群の準同型写像$f_i : N \longrightarrow M_i$が与えられたとする．このとき左$R$–加群の準同型写像$f : N \longrightarrow \prod_{i \in I} M_i$で，右図が可換となるものが唯一つ存在する．これを，**直積の普遍性**とよぶ．



$\{M_i\}_{i \in I}$を上の通りとし，直積$\prod_{i \in I} M_i$の部分集合

$$\bigoplus_{i \in I} M_i = \{(m_i) \in \prod_{i \in I} M_i \mid \text{有限個の } i \text{ 以外は } m_i = 0\}$$

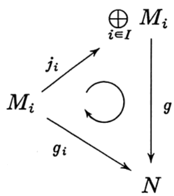
を考える．これは，直積のR–部分加群となる．また$i \in I$を固定したとき，

M_i の元 m_i に対し，i 成分が m_i で，それ以外はすべて 0 となる直和の元を対応させると，左 R-加群の準同型写像

$$j_i:\quad M_i \longrightarrow \bigoplus_{i\in I} M_i$$

ができる．$\bigoplus_{i\in I} M_i$ を左 R-加群 M_i の **直和** とよび，j_i を **標準的単射** とよぶ．

この場合も，N を左 R-加群で，$g_i: M_i \longrightarrow N$ $(i\in I)$ を左 R-加群の準同型写像とすると，$g: \bigoplus_{i\in I} M_i \longrightarrow N$ なる左 R-加群の準同型写像で，右図を可換とするものが唯一つ存在する（**直和の普遍性**）．



直積や直和の定義は，$\{M_i\}_{i\in I}$ が（Λ-）群の族のときにも意味をなし，I が有限集合のときは，共に第 II 章，§5 で定義したものと一致する．加群の場合は，和の形の方が見やすいため，直和 $\oplus$ の記号を使うことが多い．

例 1. 1 $$0 \longrightarrow M' \stackrel{f}{\longrightarrow} M \stackrel{g}{\longrightarrow} M'' \longrightarrow 0$$

を左 R-加群の短完全列とする．このとき，左 R-加群の準同型写像 $h: M'' \longrightarrow M$ で，$g\circ h = \mathrm{id}_{M''}$ となるものが存在するなら，上の完全列は **分解する** という．第 II 章，2.3 より，M の R-部分加群 M''' で，$M''' \simeq M''$，$M = f(M') + M'''$，$f(M') \cap M''' = \{0\}$ となるものが存在することと同値である．よって，第 II 章，定理 5.2 より，M の R-部分加群 M''' で，$M''' \simeq M''$，$M = f(M') \oplus M'''$ なるものが存在することと同値となる．

問 題 1. 2 M_i $(i\in I)$，N_j $(j\in J)$ を左 R-加群とするとき，

$$\mathrm{Hom}_R(\bigoplus_{i\in I} M_i,\ \prod_{j\in J} N_j) \simeq \prod_{i\in I, j\in J} \mathrm{Hom}_R(M_i, N_j)$$

が成り立つことを示せ．

1. 3 自由加群 M を左 R-加群とし，U を M の部分集合とする．このとき，

$$\sum_{1\leq i\leq n} r_i u_i \qquad (n\in \boldsymbol{N},\ r_i\in R,\ u_i\in U)$$

の形の有限和の全体は，M の R-部分加群をなす．これを $\sum_{u\in U} Ru$ または $\langle U\rangle$

で表し，Uで**生成**される（Mの）R-部分加群という．MのR-部分加群Nは，有限集合Uを適当にとると，$N=\langle U\rangle$となるとき，**有限生成**であるという．

また，UをMの部分集合とするとき，Uの任意の有限部分集合$\{u_i\}_{1\leq i\leq n}$に対し，

$$\sum r_iu_i=0 \quad (r_i\in R) \implies r_1=r_2=\cdots=r_n=0$$

が成り立つとき，UはR上**1次独立**であるという．とくに，Mの部分集合で，R上1次独立かつMを左R-加群として生成するものを，MのR上の**基底**という．Mの部分集合Uが基底となるための必要十分条件は，Mの任意の元が

$$\sum_{1\leq i\leq n} r_iu_i \qquad (n\in \boldsymbol{N},\ r_i\in R,\ \{u_i\}\subset U)$$

の形に一意的に表されることである．

左R-加群Mは，R上の基底をもつとき，**R-自由加群**であるという．$U=\{u_i\}$をMの基底とすると，

$$R\ni r \longmapsto ru_i\in Ru_i\ (\subset M)$$

は同型写像であり，Mはこれら$Ru_i\simeq R$の直和と同型となる．逆に$M=\bigoplus_i Ru_i$, $Ru_i\simeq R$ なら，$\{u_i\}$はMの基底となり，MはR-自由加群となる．R-自由加群Mの基底の濃度を，Mの**階数**とよぶ．Rが斜体または可換環のときは，階数は基底のとり方によらず定まることが証明できる．（Rが可換環の場合には，Rの極大イデアル$\mathfrak{m}$をとり，Mの代りに体$R/\mathfrak{m}$上の自由加群$(R/\mathfrak{m})\otimes_R M$を作り，$R$が体の場合に帰着させる（§2とくに問題2.7参照，階数が有限のときは補題5.3参照）．）

例 1. 3 Kを斜体とし，Mを有限生成な左K-加群（**K-ベクトル空間**）とする．Mの生成系のうち個数が最小のものを1つとり，それをUとおく．UはK上Mを生成するが，最小性より，UはK上1次独立となり，Mの基底となる．

$V=\{v_i\}_{1\leq i\leq n}$を$M$の任意の有限個の元から成る基底とする．このとき

$$M_i=Kv_1+Kv_2+\cdots+Kv_i$$

とおくと，$M_i/M_{i-1} \simeq Kv_i \simeq K$ だから，

$$M_0 = \{0\} \subset M_1 \subset M_2 \subset \cdots \subset M_{n-1} \subset M_n = M$$

は M の組成列となる．よって，ジョルダン・ヘルダーの定理（第II章，定理 8.11）より，n は（V のとり方によらず）M のみで定まる．この n を，K-ベクトル空間 M の **次元** とよぶ．M が K-加群として有限生成でないときは，M の次元は無限であるという．（M が有限生成でない場合も，左 K-加群は自由加群となり，その基底の濃度は M にのみより定まる．しかしその証明には，ツォルンの補題を必要とし，かなり面倒である．）またこの場合には組成列が存在するから，第II章，定理 8.12 より，V は左 K-加群としてネター的かつアルティン的である．

例 1. 4 M を左 R-加群とし，$U \subset M$ が R 上 M を生成するとする．各 $u \in U$ に対し，環 R を R の乗法により左 R-加群とみたものを M_u とおき，

$$L = \bigoplus_{u \in U} M_u$$

とおく．定義より，左 R-加群として $M_u \simeq R$ であり，また

$$f: \quad L = \bigoplus_{u \in U} M_u \ni (r_u) \longmapsto \sum_{u \in U} r_u \cdot u \in M$$

は，L から M の上への左 R-加群の準同型写像となる．したがって，任意の左 R-加群 M に対し，R-自由加群 L と，L より M への左 R-加群の全射な準同型 $f: L \longrightarrow M$ が存在する．

問 題 1. 5 R-自由加群は，ねじれ元をもたないことを示せ．

1. 4 次数つき加群 R を環とし，各整数 n に対して左 R-加群 M_n が与えられたとき，その直和

$$M = \bigoplus_{n \in \boldsymbol{Z}} M_n$$

を，**次数つき左 R-加群** とよぶ．このとき M_n を M の **n 次成分** といい，また $M \ni m = \sum_{n \in \boldsymbol{Z}} m_n$ $(m_n \in M_n)$ に対し，m_n を m の **n 次成分** という．

M の R-部分加群 N は，

$$N = \bigoplus_{n \in \boldsymbol{Z}} N_n \qquad (N_n \subset M_n)$$

の形のとき，**斉次（または同次）部分 R-加群** という．このとき，剰余加群

$$M/N = \bigoplus_{n \in \mathbf{Z}} (M_n/N_n)$$

も次数つき R–加群となる．

$M = \bigoplus_n M_n$，$N = \bigoplus_n N_n$ を次数つき左 R–加群とする．左 R–加群の準同型写像 $f: M \longrightarrow N$ は，条件

$$f(M_n) \subset N_{n+p} \qquad (\forall n \in \mathbf{Z})$$

を満たす p が存在するなら，p 次の **(斉次)準同型写像** であるという．このとき，f の M_n への制限を f_n で表すと，

$$\mathrm{Im}(f) = \bigoplus_n \mathrm{Im}(f_{n-p}), \qquad \mathrm{Ker}(f) = \bigoplus_n \mathrm{Ker}(f_n)$$

となり，これらは M, N の斉次部分 R–加群となる．

R を可換環とし，$A = \bigoplus_{n \in \mathbf{Z}} A_n$ を次数つき R–加群とする．このとき，A が R 上の多元環の構造をもち，しかも

$$A_p \cdot A_q \subset A_{p+q}$$

なる条件を満たすなら，A を R 上の **次数つき多元環** であるという．例えば，多項式環 $R[X]$ は次数つき多元環である．

A を R 上の次数つき多元環とする．このとき，A の斉次部分 R–加群で，部分多元環（左イデアル，右イデアル，両側イデアル）となるものを **斉次部分多元環（斉次左イデアル，斉次右イデアル，斉次両側イデアル）** という．$\mathfrak{a} = \bigoplus_{n \in \mathbf{Z}} \mathfrak{a}_n$ が A の斉次両側イデアルなら，$A/\mathfrak{a} = \bigoplus_{n \in \mathbf{Z}} (A_n/\mathfrak{a}_n)$ も次数つき多元環となる．

以上は $n \in \mathbf{Z}$ を添数にもつ場合だが，$(n_1, n_2) \in \mathbf{Z} \times \mathbf{Z}$ を添数にもつ2重次数つき加群なども，同様にして定義できる．

例 1.6 M を左 R–加群とするとき，M の R–部分加群の族 $\{F^p(M) \mid p \in \mathbf{Z}\}$ で，$F^p(M) \supset F^{p+1}(M)$ を満たすものを，M の **フィルター** とよぶ．このとき，

$$G(M) = \bigoplus_{p \in \mathbf{Z}} G^p(M), \qquad G^p(M) = F^p(M)/F^{p+1}(M)$$

は次数つき左 R–加群となる．これを F に **同伴な次数つき加群** とよぶ．

加群のフィルターにおいては，条件

$$\bigcup_p F^p(M) = M, \qquad \bigcap_p F^p(M) = \{0\}$$

を満たす場合が重要である.

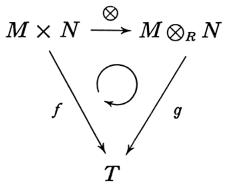
§2. テンソル積

2.1 存在と一意性　Rを環とし，Mを右R-加群，Nを左R-加群とする．このとき，直積集合$M\times N$からアーベル群Tへの写像$f: M\times N \longrightarrow T$が，

$$f(m_1+m_2, n) = f(m_1, n) + f(m_2, n)$$
$$f(m, n_1+n_2) = f(m, n_1) + f(m, n_2)$$
$$f(mr, n) = f(m, rn)$$

$(\forall m, m_1, m_2 \in M,\ \forall n, n_1, n_2 \in N,\ \forall r \in R)$ を満たすなら，fは**準双1次写像**であるという．

定理 2.1　Rを環，Mを右R-加群，Nを左R-加群とする．このとき，アーベル群$M\otimes_R N$と，$M\times N$から$M\otimes_R N$への準双1次写像$\otimes$で，次の性質を満たすものが存在する．



（1）$M\otimes_R N$は，写像$\otimes$の像で生成される．

（2）fを$M\times N$からアーベル群Tへの任意の準双1次写像とすると，アーベル群の準同型写像$g: M\otimes_R N \longrightarrow T$で，右図を可換にするものが唯一つ存在する．

$M\otimes_A N$を，MとNの**テンソル積**とよび，$(m, n)\in M\times N$の写像$\otimes$による像を$m\otimes n$で表す．Rが何か明らかなときは，$M\otimes_R N$を単に$M\otimes N$と略記する．また性質（2）を**テンソル積の普遍性**とよぶ．

［証明］　$M\times N = \{(m, n) \mid m\in M,\ n\in N\}$ で生成される自由$\boldsymbol{Z}$-加群をFとし，

$$(m_1+m_2, n) - (m_1, n) - (m_2, n)$$

$$(m, n_1 + n_2) - (m, n_1) - (m, n_2)$$
$$(mr, n) - (m, rn)$$

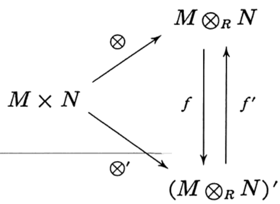
$(m, m_1, m_2 \in M,\ n, n_1, n_2 \in N,\ r \in R)$ 全体で生成される F の部分 $\boldsymbol{Z}$-加群を K で表す．F の K による剰余 $\boldsymbol{Z}$-加群を $M \otimes_R N$ で表し，自然な写像

$$M \times N \ni (m, n) \longmapsto (m, n) \ (\mathrm{mod}\, K) \in F/K = M \otimes_R N$$

を $\otimes$ で表す．このとき，$M \otimes_A N$ はアーベル群で，$\otimes : M \times N \longrightarrow M \otimes_R N$ は準双1次写像になり，$M \otimes_R N$ は写像 $\otimes$ の像で生成される．

T と f を定理の (2) のようなものとする．f は F から T へのアーベル群 ($\boldsymbol{Z}$-加群) の準同型写像 h に一意的に拡張されるが，f が準双1次写像だから，この写像 h は $\boldsymbol{Z}$-部分加群 K 上 0 となる．よって，f は写像 $g : M \otimes_R N = F/K \longrightarrow T$ で，$g \circ \otimes = f$ なるものを定める．逆に g がこの性質をもつなら，g は h より上のようにして得られることもわかる．よって定理は証明された．　　(証明終)

$\otimes' : M \times N \longrightarrow (M \otimes_R N)'$ も定理の性質をもつものとする．このとき，アーベル群の準同型写像 $f : M \otimes_R N \longrightarrow (M \otimes_R N)'$ と $f' : (M \otimes_R N)' \longrightarrow M \otimes_R N$ で，右図を可換にするものが存在する．とくに



$$(f' \circ f)(m \otimes n) = f'(m \otimes' n) = m \otimes n$$
$$(\forall m \in M, \forall n \in N)$$

が成り立つ．ところが $\otimes$ の像は $M \otimes_R N$ を生成するから，$f' \circ f = \mathrm{id}_{M \otimes N}$ が成り立つ．同様にして，$f \circ f' = \mathrm{id}_{(M \otimes N)'}$ も成り立つから，f と f' は同型で，互いに逆写像となる．この意味で，定理の性質 (1), (2) は，テンソル積 $M \otimes_R N$ と写像 $\otimes : M \times N \longrightarrow M \otimes_R N$ の組を一意的に特徴づけている．

(注) 定理 2.1 の (1) より，$M \otimes_R N$ の元は，$\sum_i m_i \otimes n_i$ $(m_i \in M,\ n_i \in N)$ の形の有限和として表される．しかし，この表現は一意的ではない．例えば，$\otimes$ の準双1次性より

$$(mr) \otimes n = m \otimes (rn) \qquad (\forall r \in R,\ \forall m \in M,\ \forall n \in N)$$

が成り立つ．

2. 2　テンソル積についての諸定義　M, M' を右 R-加群, $f : M \longrightarrow M'$ を右 R-加群の準同型写像, N, N' を左 R-加群, $g : N \longrightarrow N'$ を左 R-加群の準同型写像とする. このとき,

命 題 2. 2　(写像のテンソル積)　アーベル群の準同型写像 $f \otimes g : M \otimes_R N \longrightarrow M' \otimes_R N'$ で,

$$(f \otimes g)(m, n) = f(m) \otimes g(n)$$

$(m \in M,\ n \in N)$ を満たすものが唯一つ存在する. これを, f と g の **テンソル積** という.

$$\begin{array}{ccc} M \times N & \xrightarrow{\otimes} & M \otimes_R N \\ \downarrow{\scriptstyle (f, g)} & \circlearrowleft & \downarrow{\scriptstyle f \otimes g} \\ M' \times N' & \xrightarrow[\otimes]{} & M' \otimes_R N' \end{array}$$

[証 明]　準双 1 次写像 $h : M \times N \longrightarrow M' \otimes_R N'$ を

$$h(m, n) = f(m) \otimes g(n)$$

で定義し, これにテンソル積 $M \otimes_R N$ の普遍性を使えばよい.　　　　(証明終)

R, S, T を環とし, M を (R, S)-両側加群, N を (S, T)-両側加群とする. このとき,

$$(rm)s = r(ms), \qquad (sn)t = s(nt)$$

$(\forall m \in M,\ \forall n \in N,\ \forall r \in R,\ \forall s \in S,\ \forall t \in T)$ が成り立つ. よって

$$(r, t) : \quad M \times N \ni (m, n) \quad \longmapsto \quad (rm) \otimes (nt) \in M \otimes_S N$$

なる写像は,

$$(r(ms)) \otimes (nt) = ((rm)s) \otimes (nt) = (rm) \otimes (s(nt)) = (rm) \otimes ((sn)t)$$

を満たすから準双 1 次写像であり, テンソル積 $M \otimes_S N$ の準同型写像をひきおこす. したがって,

$$r(m \otimes n)t = (rm) \otimes (nt)$$

とおき, 両側加群の公理を一つずつチェックすることにより, テンソル積 $M \otimes_S N$ には (R, T)-両側加群の構造が入ることがわかる. よって,

命 題 2. 3　M が (R, S)-両側加群, N が (S, T)-両側加群なら, テンソル

積 $M \otimes_S N$ には，(R, T)-両側加群の構造が入る．

例えば，この命題で $T = \boldsymbol{Z}$ とおくと，M が (R, S)-両側加群で，N が左 S-加群なら，$M \otimes_S N$ には左 R-加群の構造が入ることがわかる．

R を可換環とする．このとき，左(右)R-加群は自然に右(左)R-加群となり，さらに (R, R)-両側加群ともなる（I，§7参照）．よって，命題2.3より，

系 2. 4 R を可換環，M, N を R-加群とすると，テンソル積 $M \otimes_R N$ も

$$r(m \otimes n) = (rm) \otimes n = m \otimes (rn)$$

$(r \in R,\ m \in M,\ n \in N)$ により，R-加群の構造が入る．

R, S を環とし，環の準同型写像

$$f:\quad R \longrightarrow S$$

が与えられたとする．このとき，S の加法のなすアーベル群の上には，環 S の積を使って，

$$tsr = tsf(r) \qquad \text{(左辺を右辺で定義する)}$$

$(r \in R,\ s, t \in S)$ とおくことにより，(S, R)-両側加群の構造が入る．よって，命題2.3より，

系 2. 5 （係数環の変換） M を左 R-加群とし，$f: R \longrightarrow S$ を環の準同型写像とする．このとき，テンソル積 $S \otimes_R M$ には，左 S-加群の構造が入る．これを f による **誘導加群** とよぶ．

問 題 2. 6 L を右 R-加群，M を (R, S)-両側加群，N を左 S-加群とするとき，

$$(l \otimes m) \otimes n \quad \longleftrightarrow \quad l \otimes (m \otimes n)$$

なる対応により，$(L \otimes_R M) \otimes_S N \simeq L \otimes_R (M \otimes_S N)$ となることを示せ．また L' を左 R-加群とするとき，

$$f(m \otimes n) = g(n)(m)$$

なる f と g を対応させることにより，$\mathrm{Hom}_R(M \otimes_S N, L') \simeq \mathrm{Hom}_S(N, \mathrm{Hom}_R(M, L'))$ となることを示せ．

問題2.7 M_i $(i \in I)$ を右 R-加群，N_j $(j \in J)$ を左 R-加群とする．このとき，$(\sum_i m_i) \otimes (\sum_j n_j) \longmapsto \sum_{i,j} m_i \otimes n_j$ なる対応により，

$$(\bigoplus_i M_i) \otimes_R (\bigoplus_j N_j) \simeq \bigoplus_{i,j} M_i \otimes_R N_j$$

が成り立つことを示せ．

2.3 局所化と平坦性 R を可換環，S を R の乗法的閉集合，M を R-加群とする．直積 $M \times S$ に

$$(m_1, s_1) \sim (m_2, s_2) \iff \text{ある } s \in S \text{ に対し } s(s_2 m_1 - s_1 m_2) = 0$$

という同値関係を入れ，$(m, s) \in M \times S$ の類を m/s で表す．このとき，$M_S = \{m/s \mid m \in M, s \in S\}$ は，

$$m_1/s_1 + m_2/s_2 = (s_2 m_1 + s_1 m_2)/s_1 s_2$$
$$(r/s)(m_1/s_1) = (rm_1)/(ss_1)$$

$(s_1, s_2, s \in S,\ r \in R,\ m_1, m_2 \in M)$ なる演算により，R の S による商環 R_S 上の加群となる．これを，M の S による**商加群**とよぶ（第III章，§3参照）．

$i: M \longrightarrow M_S$ なる R-加群の準同型を，$m \longmapsto m/1$ で定義する．M' も R-加群だとし，$i': M' \longrightarrow M_S'$ を同様に定義する．そこで $f \in \mathrm{Hom}_R(M, M')$ に対し，$f_S \in \mathrm{Hom}_{R_S}(M_S, M_S')$ を

$$f_S(m/s) = f(m)/s$$

$(m \in M, s \in S)$ で定義すると，これは右の可換図式を満たす．

$$\begin{array}{ccc} M & \xrightarrow{f} & M' \\ {\scriptstyle i}\downarrow & \circlearrowleft & \downarrow{\scriptstyle i'} \\ M_S & \xrightarrow[f_S]{} & M_S' \end{array}$$

商加群 M_S は，

$$(r/s) \otimes m \longmapsto (rm)/s \qquad (r \in R,\ s \in S,\ m \in M)$$

なる対応により，テンソル積 $R_S \otimes M$ と同型になる．またこの同型により，$f_S \in \mathrm{Hom}_{R_S}(M_S, M_S')$ は，写像のテンソル積 $\mathrm{id} \otimes f \in \mathrm{Hom}_R(R_S \otimes M, R_S \otimes M')$ と対応する．

命題 2.8 $M \xrightarrow{f} M' \xrightarrow{g} M''$ が R-加群の完全列なら，

$$M_S \xrightarrow{f_S} M_S' \xrightarrow{g_S} M_S''$$

は R_S-加群の完全列となる．

[証明] $g \circ f = 0$ なら，$g_S \circ f_S = (\mathrm{id} \otimes g) \circ (\mathrm{id} \otimes f) = \mathrm{id} \otimes (g \circ f) = 0$ であるから，$\mathrm{Im}\, f_S \subset \mathrm{Ker}\, g_S$ である．逆に，$m'/s \in \mathrm{Ker}\, g_S$ とすると，g_S の定義より，$g(m')/s = 0$ となる．よって，$s' \in S$ で $g(s'm') = s'g(m') = 0$ となるものが存在する．ところが $\mathrm{Im}\, f = \mathrm{Ker}\, g$ だから，$s'm' = f(m)$ なる $m \in M$ が存在する．よって

$$m'/s = (s'm')/(ss') = f(m)/(ss') = f_S(m/ss') \in \mathrm{Im}\, f_S$$

だから，$\mathrm{Im}\, f_S = \mathrm{Ker}\, g_S$ となる． (証明終)

問題 2.9 M_S を R-加群 M の商加群，N を M_S の部分 R_S-加群とする．$i: M \ni m \longmapsto m/1 \in M_S$ とするとき，$i^{-1}(N)$ は M の R-部分加群で，その商加群は N となることを示せ．(これより，M がネター的 R-加群なら，M_S もネター的 R_S-加群となることがわかる．)

命題2.8より，$R_S \otimes_R$ なるテンソル積は完全性を保つことがわかった．しかし一般のテンソル積では，完全性は保たれない．

R を（可換とは限らぬ）環とし，左 R-加群の完全列を考える．このとき，

命題 2.10 M を右 R-加群，

$$N \xrightarrow{f} N' \xrightarrow{g} N'' \longrightarrow 0$$

を左 R-加群の完全列とすると，

$$M \otimes_R N \xrightarrow{\mathrm{id} \otimes f} M \otimes_R N' \xrightarrow{\mathrm{id} \otimes g} M \otimes_R N'' \longrightarrow 0$$

も(アーベル群の)完全列となる．これを**テンソル積の右完全性**という．また上の完全列の左に 0 を補ったものが分解型完全列となるなら，下の完全列の左に 0 を補ったものも分解型完全列となる．さらに，これらにおいて，M と N を入れ替えた命題も成り立つ．

[証明] $M \otimes_R N''$ の元は，$\sum_i m_i \otimes n_i''$ $(m_i \in M,\ n_i'' \in N'')$ の形に書ける．ところが g は全射だから，$n_i'' = g(n_i')$ $(n_i' \in N')$ と書ける．よって

$$(\mathrm{id}\otimes g)(\sum_i m_i\otimes n_i') = \sum_i m_i\otimes g(n_i') = \sum_i m_i\otimes n_i''$$

となるから，$\mathrm{id}\otimes g$ も全射である．

次に，$g\circ f=0$ より $(\mathrm{id}\otimes g)\circ(\mathrm{id}\otimes f)=\mathrm{id}\otimes(g\circ f)=0$ となるから，$\mathrm{Im}(\mathrm{id}\otimes f)\subset\mathrm{Ker}(\mathrm{id}\otimes g)$ である．したがって，$L=M\otimes_R N'/\mathrm{Im}(\mathrm{id}\otimes f)$ とおくと，$\mathrm{id}\otimes g$ は

$$h:\quad L\longrightarrow M\otimes_R N''$$

なる全射をひきおこす．この写像の逆写像を作るため，N'' の元 n'' に対し $n''=g(n')$ なる $n'\in N'$ をとり，

$$i:\quad M\times N''\ni(m,n'')\longmapsto m\otimes n'\ (\mathrm{mod}\ \mathrm{Im}(\mathrm{id}\otimes f))\in L$$

とおく．ここで，$n_1'\in N'$ も $n''=g(n_1')$ を満たしたとすると，$g(n'-n_1')=n''-n''=0$ より，$n'-n_1'=f(n)$ $(n\in N)$ と書ける．よって $m\otimes n'\equiv m\otimes n_1'$ (mod $\mathrm{Im}(\mathrm{id}\otimes f)$) となり，$i$ は n' のとり方によらずに定まっている．i が準双1次写像となることは，定義より明らかだから，テンソル積の普遍性より，準同型

$$j:\quad M\otimes_R N''\longrightarrow L$$

で，$j(m\otimes n'')=m\otimes n'$ (mod $\mathrm{Im}(\mathrm{id}\otimes f)$) を満たすものが存在する．これは $h:L\longrightarrow M\otimes_R N''$ の逆写像を与えるから，h は同型となり，$\mathrm{Im}(\mathrm{id}\otimes f)=\mathrm{Ker}(\mathrm{id}\otimes g)$ となる．

次に

$$0\longrightarrow N\xrightarrow{f}N'\xrightarrow{g}N''\longrightarrow 0$$

が完全列で，$k:N''\longrightarrow N'$ なる準同型写像で $g\circ k=\mathrm{id}_{N''}$ なるものが存在したとする．このとき $(\mathrm{id}_M\otimes g)\circ(\mathrm{id}_M\otimes k)=\mathrm{id}_M\otimes(g\circ k)=\mathrm{id}_M\otimes\mathrm{id}_{N''}=\mathrm{id}_{M\otimes N''}$ が成り立つ．よって

$$0\longrightarrow M\otimes_R N\xrightarrow{\mathrm{id}\otimes f}M\otimes_R N'\xrightarrow{\mathrm{id}\otimes g}M\otimes_R N''\longrightarrow 0$$

も分解型完全列となる．

M と N を入れ替えてもよいことは，以上の証明より明らかである．（証明終）

M を右 R-加群とする．このとき，任意の左 R-加群の完全列

$$0\longrightarrow N\xrightarrow{f}N'\xrightarrow{g}N''\longrightarrow 0$$

に対し，これより作られる列

$$0 \longrightarrow M \otimes_R N \xrightarrow{\mathrm{id}\otimes f} M \otimes_R N' \xrightarrow{\mathrm{id}\otimes g} M \otimes_R N'' \longrightarrow 0$$

も（アーベル群の）完全列となるなら，M を **平坦** であるという．左 R-加群に対する平坦性も同様に定義する．

例 2. 11 命題 2.8 より商環 R_S は R-加群として平坦である．他方，$R = \boldsymbol{Z}$, $M = \boldsymbol{Z}/2\boldsymbol{Z}$ とし，

$$f: \quad \boldsymbol{Z} \ni a \longmapsto 2a \in \boldsymbol{Z}, \qquad g: \quad \boldsymbol{Z} \ni b \longmapsto b \pmod 2 \in \boldsymbol{Z}/2\boldsymbol{Z}$$

とする．このとき

$$0 \longrightarrow \boldsymbol{Z} \xrightarrow{f} \boldsymbol{Z} \xrightarrow{g} \boldsymbol{Z}/2\boldsymbol{Z} \longrightarrow 0$$

は完全だが，$\mathrm{id} \otimes f: (\boldsymbol{Z}/2\boldsymbol{Z}) \otimes_{\boldsymbol{Z}} \boldsymbol{Z} \longrightarrow (\boldsymbol{Z}/2\boldsymbol{Z}) \otimes_{\boldsymbol{Z}} \boldsymbol{Z}$ は

$$(\mathrm{id} \otimes f)(\sum_i c_i \otimes d_i) = \sum_i c_i \otimes 2d_i = \sum_i 2c_i \otimes d_i = \sum_i 0 \otimes d_i = 0$$

となり，零写像となる．よって，$\boldsymbol{Z}$-加群 $\boldsymbol{Z}/2\boldsymbol{Z}$ は平坦ではない．

一般に，R を可換環，M を（右）R-加群とし，M がねじれ元 $m \neq 0$ をもつとする．そこで，R の零因子でない元 $r \neq 0$ が $mr = 0$ を満たすものとし，$f: R \ni a \longmapsto ra \in R$ とおく．R は可換だから f は左 R-加群の準同型であり，r は零因子ではないから f は単射である．したがって $0 \longrightarrow R \xrightarrow{f} R \longrightarrow R/rR \longrightarrow 0$ は（左）R-加群の完全列となるが，$\mathrm{id} \otimes f: M \otimes_R R \longrightarrow M \otimes_R R$ は，$m \otimes 1 \neq 0$ かつ $(\mathrm{id} \otimes f)(m \otimes 1) = m \otimes r = mr \otimes 1 = 0$ となるから単射でない．よって M は平坦ではない．いい直すと，可換環 R 上の R-加群 M が平坦なら，M は 0 以外ねじれ元をもたない．

2. 4 テンソル代数 R を可換環とし，M を R-加群とする．$T^0(M) = R$ とおき，自然数 p に対し，

$$T^p(M) = M \otimes_R M \otimes_R \cdots \otimes_R M \qquad (p \text{ 個のテンソル積})$$

とおく．R は可換だから，R-加群 M は (R, R)-両側加群の構造をもち，したがって，$T^p(M)$ は R-加群の構造をもつ（系 2.4 参照）．定義より明らかに，$T^p(M)$ は

$$a_{i_1} \otimes a_{i_2} \otimes \cdots \otimes a_{i_p} \qquad (a_{i_1}, a_{i_2}, \cdots, a_{i_p} \in M)$$

の形の元全体で生成されるが，とくに M が $\{u_i\}_{i \in I}$ を基底としてもつ R-自由加群なら，$T^p(M)$ は $\{u_{i_1} \otimes u_{i_2} \otimes \cdots \otimes u_{i_p} \mid i_1, i_2, \cdots, i_p \in I\}$ を基底とする

R–自由加群となる（問題 2.7 参照）.

一般に

$$T(M)=\bigoplus_{p\geqq 0}T^p(M)$$

とおき，

$$(a_{i_1}\otimes a_{i_2}\otimes\cdots\otimes a_{i_p})\otimes(b_{j_1}\otimes b_{j_2}\otimes\cdots\otimes b_{j_q})$$
$$=a_{i_1}\otimes a_{i_2}\otimes\cdots\otimes a_{i_p}\otimes b_{j_1}\otimes b_{j_2}\otimes\cdots\otimes b_{j_q}$$

で積 $\otimes$: $T^p(M)\times T^q(M)\longrightarrow T^{p+q}(M)$ $(p,q\geqq 0)$ を定義する．このとき $T(M)=\bigoplus_p T^p(M)$ は，R 上の次数つき多元環となる．これを M 上の **テンソル代数** とよぶ．

環 $T(M)$ において，$m\otimes m$ $(m\in M)$ 全体で生成される両側イデアルを $\mathfrak{a}$ とする．これは $T(M)$ の斉次両側イデアルをなし，その剰余環 $T(M)/\mathfrak{a}$ を $\wedge(M)$ で表すと，これは次数つき多元環をなす．$\wedge(M)$ を M 上の **外積代数** とよび，その積を $\wedge$ で表す．$\mathfrak{a}$ は斉次イデアルだから，$\wedge(M)=T(M)/\mathfrak{a}$ も次数つき多元環となり，$\wedge(M)=\bigoplus_{p\geqq 0}\wedge^p(M)$ と書ける．

$\mathfrak{a}$ の 1 次成分 $\mathfrak{a}_1$ は $\{0\}$ だから，R–加群の準同型写像

$$M\ni m \longmapsto m \pmod{\mathfrak{a}}\in\wedge(M)$$

は単射である．よって $\wedge^1(M)\simeq M$ となるから，$\wedge^1(M)$ と M を同一視する．

$a,b\in M$ とする．このとき

$$a\otimes b+b\otimes a=(a+b)\otimes(a+b)-a\otimes a-b\otimes b\in\mathfrak{a}$$

となる．よって $\wedge(M)$ において，

$$a\wedge b=-b\wedge a$$

が成り立つ．

$T^p(M)$ は $a_{i_1}\otimes a_{i_2}\otimes\cdots\otimes a_{i_p}$ $(a_{i_1},a_{i_2},\cdots,a_{i_p}\in M)$ の形の元全体で R–加群として生成されるから，$\wedge(M)=T(M)/\mathfrak{a}$ の p 次成分 $\wedge^p(M)=T^p(M)/\mathfrak{a}_p$ は，

$$a_{i_1}\wedge a_{i_2}\wedge\cdots\wedge a_{i_p}\qquad(a_{i_1},a_{i_2},\cdots,a_{i_p}\in M)$$

の形の元全体により R-加群として生成される．これより，

$$u \wedge v = (-1)^{pq} v \wedge u \qquad (u \in \wedge^p(M),\ v \in \wedge^q(M))$$

が成り立つことがわかる．

M, N を R-加群とし，$f: M \longrightarrow N$ を準同型写像とする．このとき，

$$T(f)\ (m_1 \otimes m_2 \otimes \cdots \otimes m_p) = f(m_1) \otimes f(m_2) \otimes \cdots \otimes f(m_p)$$

$$(m_1, m_2, \cdots, m_p \in M)$$

とおくことにより，次数つき多元環の間の 0 次の準同型写像

$$T(f): \quad T(M) \longrightarrow T(N)$$

が定義される．さらに，$T(f)$ は

$$\wedge(f)\ (m_1 \wedge m_2 \wedge \cdots \wedge m_p) = f(m_1) \wedge f(m_2) \wedge \cdots \wedge f(m_p)$$

$$(m_1, m_2, \cdots, m_p \in M)$$

を満たす次数つき多元環の準同型写像

$$\wedge(f): \quad \wedge(M) \longrightarrow \wedge(N)$$

をひきおこす．

例 2. 12 M を基底 $\{u_i\}_{1 \leq i \leq n}$ をもつ階数 n の R-自由加群とする．このとき問題 2.7 より，$T^p(M)$ は $u_{i_1} \otimes u_{i_2} \otimes \cdots \otimes u_{i_p}$ $(1 \leqq i_1, i_2, \cdots, i_p \leqq n)$ を基底とする R-自由加群となる．ところが $\wedge(M)$ において，$m_1 \wedge m_2 = -m_2 \wedge m_1$ $(m_1, m_2 \in M)$ なる公式が成り立つから，$u_{i_1} \wedge u_{i_2} \wedge \cdots \wedge u_{i_p}$ $(1 \leqq i_1 < i_2 < \cdots < i_p \leqq n)$ の形の元が R-加群として $\wedge(M)$ を生成する．ここで，

$$\sum_{1 \leq i_1 < i_2 < \cdots < i_p \leq n} r_{i_1 i_2 \cdots i_p} u_{i_1} \otimes u_{i_2} \otimes \cdots \otimes u_{i_p} \qquad (r_{i_1 i_2 \cdots i_p} \in R)$$

の形の元で，$m \otimes m$ $(\forall m \in M)$ で生成する $T(M)$ のイデアル $\mathfrak{a}$ に属するのは 0 に限ることは，条件 $i_1 < i_2 < \cdots < i_p$ より明らかである．したがって，R-加群として，

$$\wedge(M) = \bigoplus_{1 \leq i_1 < i_2 < \cdots < i_p \leq n} R u_{i_1} \wedge u_{i_2} \wedge \cdots \wedge u_{i_p}$$

となる．とくに $\wedge^p(M)$ は，$\{u_{i_1} \wedge u_{i_2} \wedge \cdots \wedge u_{i_p} \mid 1 \leqq i_1 < i_2 < \cdots < i_p \leqq n\}$ を基底とする階数 $\binom{n}{p}$ の R-自由加群となる．

$f: M \longrightarrow M$ を R-加群の自己準同型とする．このとき $\wedge^n(M) = R u_1 \wedge u_2 \wedge \cdots \wedge u_n$ であるから，f は

$$\wedge(f): \quad R u_1 \wedge u_2 \wedge \cdots \wedge u_n \longrightarrow R u_1 \wedge u_2 \wedge \cdots \wedge u_n$$

なる R-加群の自己準同型をひきおこす．よって

$$\wedge(f)\, u_1 \wedge u_2 \wedge \cdots \wedge u_n = \det(f)\, u_1 \wedge u_2 \wedge \cdots \wedge u_n \qquad (\exists \det(f) \in R)$$

と書ける．この $\det(f)$ は，基底 $\{u_i\}$ を使って f を行列表現したときの，第 I 章，§10 の意味での行列式と一致する．このことは，

$$(\sum_{i_1} a_{1i_1}u_{i_1}) \wedge (\sum_{i_2} a_{2i_2}u_{i_2}) \wedge \cdots \wedge (\sum_{i_n} a_{ni_n}u_{i_n})$$

$(1 \leqq i_1, i_2, \cdots, i_n \leqq n)$ なる和を $\det(f)\ u_1 \wedge u_2 \wedge \cdots \wedge u_n$ の形に変形すると，$\det(f)$ が行列式の定義と一致することからわかる．

問題 2. 13 M を R-加群とし，テンソル代数 $T(M)$ を $m_1 \otimes m_2 - m_2 \otimes m_1$ $(m_1, m_2 \in M)$ の形の元全体で生成される両側イデアルで割った剰余環を $S(M)$ で表し，M 上の **対称代数** とよぶ．M が階数 n の R-自由加群なら，$S(M)$ は多項式環 $R[x_1, x_2, \cdots, x_n]$ と同型となることを示せ．

問題 2. 14 R を可換環とし，A, B を R 上の次数つき多元環とする．このとき，テンソル積 $A \otimes_R B$ に

$$(a_1 \otimes b_1)\cdot(a_2 \otimes b_2) = (-1)^{q_1p_2} a_1a_2 \otimes b_1b_2 \qquad (a_i \in A_{p_i},\ \ b_i \in B_{q_i})$$

で積を定義すると，$A \otimes_R B$ も次数つき多元環となることを示せ．とくに，外積代数について，次数つき多元環として，

$$\wedge(M_1 \oplus M_2) \simeq \wedge(M_1) \otimes \wedge(M_2)$$

が成り立つことを示せ．

§3. 射影加群と入射加群

3. 1 Hom_R の左完全性 R を環とし，M, N を左 R-加群，$\mathrm{Hom}_R(M, N)$ を左 R-加群の準同型写像 $f: M \longrightarrow N$ 全体のなすアーベル群とする．

M', N' を左 R-加群とし，$g: M' \longrightarrow M$，$h: N \longrightarrow N'$ を左 R-加群の準同型写像とする．このとき，写像の合成

$$f \longmapsto f\circ g, \qquad f \longmapsto h\circ f$$

により，写像

$$g^*: \quad \mathrm{Hom}_R(M, N) \longrightarrow \mathrm{Hom}_R(M', N),$$

$$h_*: \quad \mathrm{Hom}_R(M, N) \longrightarrow \mathrm{Hom}_R(M, N')$$

が定義される．これらはアーベル群の準同型写像であり，$g' \in \mathrm{Hom}_R(M'', M')$ と $h' \in \mathrm{Hom}_R(N', N'')$ に対し，

$$(g' \circ g)^* = g^* \circ (g')^*, \qquad (h' \circ h)_* = (h')_* \circ h_*$$

を満たす．

命題 3.1 M を左 R-加群，

$$0 \longrightarrow N \xrightarrow{f} N' \xrightarrow{g} N''$$

を左 R-加群の完全列とする．このとき

$$0 \longrightarrow \mathrm{Hom}_R(M, N) \xrightarrow{f_*} \mathrm{Hom}_R(M, N') \xrightarrow{g_*} \mathrm{Hom}_R(M, N'')$$

も，アーベル群の完全列となる．さらに，上の列の右に 0 を補ったものが分解型完全列（例 1.1 参照）となるなら，下の列の右に 0 を補ったものも分解型完全列となる．

同様に，

命題 3.2 $$M \xrightarrow{f} M' \xrightarrow{g} M'' \longrightarrow 0$$

を左 R-加群の完全列，N を左 R-加群とする．このとき

$$0 \longrightarrow \mathrm{Hom}_R(M'', N) \xrightarrow{g^*} \mathrm{Hom}_R(M', N) \xrightarrow{f^*} \mathrm{Hom}_R(M, N)$$

もアーベル群の完全列となる．さらに，上の列の左に 0 を補ったものが分解型完全列となるなら，下の列の右に 0 を補ったものも分解型完全列となる．

これらの性質を，**Hom_R の左完全性** という．

[**証明**] どちらの証明も大体同じなので，命題 3.1 のみを証明する．

$h \in \mathrm{Hom}_R(M, N)$ とする．もし $f_*(h) = f \circ h = 0$ なら，すべての $m \in M$ に対して $f(h(m)) = 0$ となる．ところが f は単射だから，$h(m) = 0$ となり，$h = 0$ となる．したがって f_* も単射である．

次に，$g \circ f = 0$ だから，$g_* \circ f_* = (g \circ f)_* = 0$ となる．よって $\mathrm{Im}(f_*) \subset \mathrm{Ker}(g_*)$ が成り立つ．逆に $i \in \mathrm{Hom}_R(M, N')$ が $g_*(i) = g \circ i = 0$ を満たしたとする．このとき，すべての $m \in M$ に対し，$g(i(m)) = 0$ となる．ところが $\mathrm{Im}(f) \supset \mathrm{Ker}(g)$ だか

ら，$i(m)=f(n)$ $(n\in N)$ と書ける．ここで f は単射だから，$n\in N$ は $m\in M$ より一意的に定まる．よって $j: M\longrightarrow N$ を $j(m)=n$ で定義する．この j は，定義より，$i=f\circ j$ を満たす．

$j(m_l)=n_l$ $(l=1,2)$ だとする．このとき

$$i(m_1+m_2)=i(m_1)+i(m_2)=f(n_1)+f(n_2)=f(n_1+n_2)$$

であるから，$j(m_1+m_2)=j(m_1)+j(m_2)$ $(m_1,m_2\in M)$ が成り立つ．同様にして $j(r\cdot m)=r\cdot j(m)$ $(r\in R,\ m\in M)$ が成り立つこともわかり，$j\in \mathrm{Hom}_R(M,N)$ となる．ところが $i=f\circ j$ だから，$i=f_*(j)\in \mathrm{Im}(f_*)$ となり，$\mathrm{Im}(f_*)=\mathrm{Ker}(g_*)$ が成り立つ．

命題の後半を示すため，

$$0\longrightarrow N\xrightarrow{f}N'\xrightarrow{g}N''\longrightarrow 0$$

が完全列で，$k: N''\longrightarrow N'$ が $g\circ k=\mathrm{id}_{N''}$ を満たすとする．このとき $k_*: \mathrm{Hom}_R(M,N'')\longrightarrow \mathrm{Hom}_R(M,N')$ は，

$$g_*\circ k_*=(g\circ k)_*=(\mathrm{id}_{N''})_*=\mathrm{id}_{\mathrm{Hom}_R(M,N'')}$$

を満たす．よって

$$0\longrightarrow \mathrm{Hom}_R(M,N)\xrightarrow{f_*}\mathrm{Hom}_R(M,N')\xrightarrow{g_*}\mathrm{Hom}_R(M,N'')\longrightarrow 0$$

は分解型完全列となる．　　　　　　　　　　　　　　　　　　（証明終）

3.2　射影加群と入射加群　　M を左 R–加群とする．このとき，左 R–加群の任意の完全列

$$0\longrightarrow N\xrightarrow{f}N'\xrightarrow{g}N''\longrightarrow 0$$

に対して，これよりひきおこされる

$$0\longrightarrow \mathrm{Hom}_R(M,N)\xrightarrow{f_*}\mathrm{Hom}_R(M,N')\xrightarrow{g_*}\mathrm{Hom}_R(M,N'')\longrightarrow 0$$

が（アーベル群の）完全列となるなら，M は **射影的** であるという（命題 3.1 参照）．これについて，次のような特徴づけができる．

命 題 3.3　左 R–加群 M について，次は同値である．

（1）　M は射影的である．

（2）　$h: N\longrightarrow N'$ なる準同型写像が全射なら，

$$h_*:\quad \mathrm{Hom}_R(M,N)\longrightarrow \mathrm{Hom}_R(M,N')$$

も全射となる.

（3） M はある R-自由加群の直和因子となる. つまり, ある左 R-加群 M' があり, $M \oplus M'$ が R-自由加群となる.

[証 明] （1）$\Longrightarrow$（2）　$0 \longrightarrow \mathrm{Ker}(h) \longrightarrow N \xrightarrow{h} N' \longrightarrow 0$ が完全列だから, 射影加群の定義より, h_* も全射となる.

（2）$\Longrightarrow$（3）　例 1.4 より, R-自由加群 F と, F から M の上への準同型写像 f : $F \longrightarrow M$ が存在する. f は全射だから, $f: F \longrightarrow M$ に (2) を使うと, $g: M \longrightarrow F$ なる準同型写像で, $f \circ g = f_*(g) = \mathrm{id}_M$ となるものが存在することがわかる. よって $F \simeq \mathrm{Ker}(f) \oplus M$ となる (例 1.1 参照).

（3）$\Longrightarrow$（1）　M' が左 R-加群で, $F = M \oplus M'$ が R-自由加群になったとする. F の基底を $\{u_i\}_{i \in I}$ とし, $\pi: F \longrightarrow M$ を射影, $h: M \longrightarrow F$ をうめ込みとする. $0 \longrightarrow N \xrightarrow{f} N' \xrightarrow{g} N'' \longrightarrow 0$ を任意の左 R-加群の短完全列とする. このとき, g は全射だから, 任意の $j \in \mathrm{Hom}_R(M, N'')$ に対して, $n_i' \in N'$ で, $g(n_i') = j(\pi(u_i))$ を満たすものが存在する. そこで

$$k(\sum_i r_i u_i) = \sum_i r_i n_i'$$

で $k \in \mathrm{Hom}_R(F, N')$ を定義する. これは $\{u_i\}_{i \in I}$ が自由加群の基底だから, 左 R-加群の準同型写像を定めている. 定義より明らかに, g は $g \circ k = j \circ \pi$ を満たす. よって $l = k \circ h \in \mathrm{Hom}_R(M, N')$ は,

$$g_*(l) = g \circ l = g \circ k \circ h = j \circ \pi \circ h = j \circ \mathrm{id}_M = j$$

を満たす. よって $g_*: \mathrm{Hom}_R(M, N') \longrightarrow \mathrm{Hom}_R(M, N'')$ は全射であり, (1) が成り立つ.　(証明終)

M を左 R-加群とする. このとき, 左 R-加群の任意の完全列

$$0 \longrightarrow N \xrightarrow{f} N' \xrightarrow{g} N'' \longrightarrow 0$$

に対して, これよりひきおこされる

$$0 \longrightarrow \mathrm{Hom}_R(N'', M) \xrightarrow{g^*} \mathrm{Hom}_R(N', M) \xrightarrow{f^*} \mathrm{Hom}_R(N, M) \longrightarrow 0$$

が完全列となるなら, M を **入射的** であるという. 入射加群についても, 命題 3.3 と同様にして, 次の命題が証明できる.

命 題 3.4 左 R-加群 M について, 次は同値である.

（1）　M は入射的である．

（2）　$h : N \longrightarrow N'$ なる準同型写像が単射なら，

$$h^* : \quad \mathrm{Hom}_R(N', M) \longrightarrow \mathrm{Hom}_R(N, M)$$

は全射となる．

例 3．5　　$0 \longrightarrow M_1 \xrightarrow{f} M_2 \xrightarrow{g} M_3 \longrightarrow 0$

を左 R–加群の短完全列とする．このとき，M_3 が射影的なら，命題 3.3 の（3）を $g_* : \mathrm{Hom}_R(M_3, M_2) \longrightarrow \mathrm{Hom}_R(M_3, M_3)$ に適用すると，$i \in \mathrm{Hom}_R(M_3, M_2)$ で $g_*(i) = g \circ i = \mathrm{id}_{M_3}$ となるものが存在することがわかる．よって，上の完全列は分解し，$M_2 \simeq M_1 \oplus M_3$ となる．

同様にして，M_1 が入射的なら，$j \in \mathrm{Hom}_R(M_2, M_1)$ で $j \circ f = \mathrm{id}_{M_1}$ なるものが存在する．したがって，

$$\mathrm{Im}(f) \simeq M_1, \qquad \mathrm{Im}(f) + \mathrm{Ker}(j) = M_2, \qquad \mathrm{Im}(f) \cap \mathrm{Ker}(j) = \{0\}$$

が成り立つから，$M_2 = \mathrm{Im}(f) \oplus \mathrm{Ker}(j)$，$\mathrm{Im}(f) \simeq M_1$，$\mathrm{Ker}(j) \simeq M_3$ と直和に分解される．いい直すと，この場合にも上の短完全列は分解し，$M_2 \simeq M_1 \oplus M_3$ となる．とくに，入射加群は，それを含む任意の加群の直和因子となることがわかる．

例 3．6　M を射影的左 R–加群とし，M は R–自由加群 F の直和因子であるとする．F の基底を $\{u_i\}_{i \in I}$ とし，$i : M \longrightarrow F$ をうめ込みとする．

（♯）　$0 \longrightarrow N \xrightarrow{f} N' \xrightarrow{g} N'' \longrightarrow 0$

を任意の右 R–加群の短完全列とし，これより導かれる

（♭）　$0 \longrightarrow N \otimes_R M \xrightarrow{f \otimes \mathrm{id}} N' \otimes_R M \xrightarrow{g \otimes \mathrm{id}} N'' \otimes_R M \longrightarrow 0$

を考える．

$$\begin{array}{ccc} N \otimes_R M & \xrightarrow{f \otimes \mathrm{id}_M} & N' \otimes_R M \\ \downarrow{\scriptstyle \mathrm{id}_N \otimes i} & \circlearrowright & \downarrow{\scriptstyle \mathrm{id}_{N'} \otimes i} \\ N \otimes_R F & \xrightarrow[f \otimes \mathrm{id}_F]{} & N' \otimes_R F \end{array}$$

問題 2.7 より，

$$N \otimes_R F = N \otimes \Big(\bigoplus_{i \in I} R u_i \Big) \simeq \bigoplus_{i \in I} N \otimes_R u_i$$

となるから，$f \otimes \mathrm{id}_F : N \otimes_R F \longrightarrow N' \otimes_R F$ は，$f : N \longrightarrow N'$ なる写像の $\#(I)$ 個のコピーであると思える．ところが f は単射だから，$f \otimes \mathrm{id}_F$ も単射である．次に，左 R–加群として $F = M \oplus M'$ だとすると，問題 2.7 より，$N \otimes_R F \simeq N \otimes_R M \oplus N \otimes_R M'$ となる．$\mathrm{id}_N \otimes i : N \otimes_R M \longrightarrow N \otimes_R F$ は，この直和分解に対応するうめ込みだから，単射となる．したがって，上の図の可換性より，$f \otimes \mathrm{id}_M : N \otimes_R$

$M \longrightarrow N' \otimes_R M$ も単射となる．よって，命題2.10より，(♯)が完全列なら(♭)も完全列となる．これより，射影加群は平担であることがわかる．

3.3　双対加群　R を環とし，R の乗法により R 自身を左 R-加群と思う．このとき，任意の左 R-加群 M に対し，

$$M^* = \mathrm{Hom}_R(M, R)$$

は，

$$(f \cdot r)(m) = f(m) \cdot r \qquad (f \in \mathrm{Hom}_R(M, R),\ r \in R,\ m \in M)$$

とおくことにより，右 R-加群となる．M^* を M の **双対加群** とよび，その元を M 上の **1次形式** という．

M, N を左 R-加群とし，$f: M \longrightarrow N$ を左 R-加群の準同型写像とする．このとき，${}^t f: N^* \longrightarrow M^*$ を

$$({}^t f(\xi))(m) = \xi(f(m)) \qquad (\xi \in N^* = \mathrm{Hom}_R(N, R),\ m \in M)$$

と定義すると，${}^t f$ は右 R-加群の準同型写像となる．これを **転置写像** とよぶ．

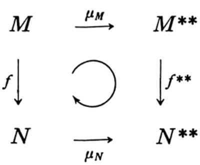
右 R-加群に対しても同様のことを行うと，その双対加群として，左 R-加群ができる．とくに，左 R-加群 M の双対加群 M^* は右 R-加群だから，M^* の双対加群 M^{**} は左 R-加群となる．このとき，$m \in M$ に対して，

$$m^{**}(\xi) = \xi(m) \qquad (\xi \in M^* = \mathrm{Hom}_R(M, R))$$

とおくと，m^{**} は $M^{**} = \mathrm{Hom}_R(M^*, R)$ の元となる．そこで

$$\mu_M: \quad M \longrightarrow M^{**}$$

を $m \longmapsto m^{**}$ で定義すると，μ_M は左 R-加群の準同型写像となる．



左 R-加群の準同型写像 $f: M \longrightarrow N$ は，右 R-加群の準同型写像 ${}^t f: N^* \longrightarrow M^*$ をひきおこす．したがって，${}^t f$ の転置写像は，左 R-加群の準同型写像 ${}^t({}^t f): M^{**} \longrightarrow N^{**}$ をひきおこす．これを f^{**} で表すと，

$$(f^{**})(m^{**})(\eta) = m^{**}({}^t f(\eta)) = {}^t f(\eta)(m) = \eta(f(m)) = (f(m))^{**}(\eta)$$

$(m \in M,\ \eta \in N^*)$ が成り立つ．これは前ページの図の可換性を意味する．

例 3.7 問題 1.2 より，

$$(\bigoplus_{i \in I} M_i)^* \simeq \prod_{i \in I} M_i^*$$

が成り立つ．とくに，I を有限集合 $\{1, 2, \cdots, n\}$ とすると，

$$(\bigoplus_{1 \leq i \leq n} M_i)^* \simeq \bigoplus_{1 \leq i \leq n} M_i^*$$

が成り立つ．また $\xi \in R^* = \mathrm{Hom}_R(R, R)$ に対し，

$$\xi(r) = \xi(r \cdot 1) = r \cdot \xi(1) \qquad (r \in R)$$

が成り立つから，

$$R^* \ni \xi \longmapsto \xi(1) \in R$$

は，右 R-加群の同型写像をなす．したがって，M が階数 n $(n \in \boldsymbol{N})$ の R-自由加群なら，M^* も階数 n の R-自由加群となる．

さて，$R = \boldsymbol{Z}$, $M = \boldsymbol{Z}/2\boldsymbol{Z}$ なら，$M^* \simeq \mathrm{Hom}_{\boldsymbol{Z}}(\boldsymbol{Z}/2\boldsymbol{Z}, \boldsymbol{Z}) = \{0\}$ となる．したがって，μ_M は一般には同型とはならない．しかし次の場合には，μ_M は同型となる．

定理 3.8 M が有限生成射影加群なら，M^* も有限生成射影加群で，μ_M : $M \longrightarrow M^{**}$ は左 R-加群の同型となる．

［証明］ M の有限個の生成元を $\{m_i\}_{1 \leq i \leq n}$ とし，$F = R \oplus \cdots \oplus R$ を階数 n の R-自由加群とする．このとき

$$f: \quad F = R \oplus \cdots \oplus R \ni (r_1, \cdots, r_n) \quad \longmapsto \sum_{1 \leq i \leq n} r_i m_i \in M$$

は，左 R-加群の全射をなす．したがって，M は射影的だから $F \simeq M \oplus M'$ となる．よって，例 3.7 より，$F^* \simeq M^* \oplus (M')^*$ も階数 n の R-自由加群となる．とくに F^* は n 個の元で生成されるから，M^* も n 個の元で生成される射影加群となる．

また $\mu_F : F = M \oplus M' \longrightarrow F^{**} = M^{**} \oplus (M')^{**}$ は直和分解を保つ同型だから，それの M への制限 $\mu_M : M \longrightarrow M^{**}$ も同型となる．（証明終）

問題 3.9 R を可換環とし，$M_1, M_2, \cdots, M_n$ を有限生成射影 R-加群とする．このとき，$M_1 \otimes_R M_2 \otimes_R \cdots \otimes_R M_n$ も有限生成射影加群で，

$$M_1^* \otimes_R M_2^* \otimes_R \cdots \otimes_R M_n^* \simeq (M_1 \otimes_R M_2 \otimes_R \cdots \otimes_R M)^*$$

が成り立つことを示せ．

§4. ホモロジー*

この§では，複体とそのホモロジーについて調べる．この§の結果は，以後では使わない．

4.1 複体とホモロジー R を環とする．次数つき左 R-加群 $C=\bigoplus_{n\in\boldsymbol{Z}}C_n$ と，C の -1 次の自己準同型写像 $\partial=\{\partial_n: C_n \longrightarrow C_{n-1}\}$ の組で，

$$\partial_n\circ\partial_{n+1}=0 \qquad (\forall n\in\boldsymbol{Z})$$

を満たすものを（鎖）**複体** という（1.4参照）：

$$\cdots\longrightarrow C_{n+1}\xrightarrow{\partial_{n+1}}C_n\xrightarrow{\partial_n}C_{n-1}\longrightarrow\cdots$$

このとき，$\mathrm{Ker}(\partial)$ および $\mathrm{Im}(\partial)$ を **輪体加群** および **境界加群** とよび，$Z(C)$ および $B(C)$ で表す．これらは明らかに C の斉次部分 R-加群をなし，条件 $\partial_n\circ\partial_{n+1}=0$ より，$Z(C)\supset B(C)$ を満たす．そこで，剰余加群 $Z(C)/B(C)=\bigoplus_{n\in\boldsymbol{Z}}Z_n(C)/B_n(C)$ を $H(C)=\bigoplus_{n\in\boldsymbol{Z}}H_n(C)$ と表し，(C,∂) の **ホモロジー（加）群** という．

(C,∂) を複体とするとき，C の斉次部分 R-加群 $D=\bigoplus_{n\in\boldsymbol{Z}}D_n$ で，$\partial_n(D_n)\subset D_{n-1}$ を満たすものを，**部分複体** という．D が (C,∂) の部分複体なら，$\partial=\{\partial_n\}$ は剰余加群 $C/D=\bigoplus_{n\in\boldsymbol{Z}}C_n/D_n$ の -1 次の準同型 $\bar{\partial}=\{\bar{\partial}_n\}$ をひきおこし，$\bar{\partial}$ は $\bar{\partial}_n\circ\bar{\partial}_{n+1}=0$ を満たす．この複体 $(C/D,\bar{\partial})$ を **剰余複体** という．

(C,∂) と (C',∂') を複体とするとき，次数つき左 R-加群としての 0 次の準同型写像 $f=\{f_n: C_n\longrightarrow C_n'\}$ で，図式

$$\begin{array}{ccccccccc}
\cdots\longrightarrow & C_{n+1} & \xrightarrow{\partial_{n+1}} & C_n & \xrightarrow{\partial_n} & C_{n-1} & \longrightarrow\cdots \\
 & \big\downarrow{\scriptstyle f_{n+1}} & & \big\downarrow{\scriptstyle f_n} & & \big\downarrow{\scriptstyle f_{n-1}} & \\
\cdots\longrightarrow & C_{n+1}' & \xrightarrow{\partial_{n+1}'} & C_n' & \xrightarrow{\partial_n'} & C_{n-1}' & \longrightarrow\cdots
\end{array}$$

を可換とするものを，**複体写像** という．このとき，$\mathrm{Ker}(f)=\bigoplus_{n\in\boldsymbol{Z}}\mathrm{Ker}(f_n)$ は C の部分複体をなし，$\mathrm{Im}(f)=\bigoplus_{n\in\boldsymbol{Z}}\mathrm{Im}(f_n)$ は C' の部分複体をなす．

$f: C \longrightarrow C'$ を複体写像とする．$Z_n(C) = Z_n$，$B_n(C) = B_n$ などとおくと，可換性 $\partial_n' \circ f_n = f_{n-1} \circ \partial_n$，$\partial_{n+1}' \circ f_{n+1} = f_n \circ \partial_{n+1}$ より，

$$f_n(Z_n) \subset Z_n', \qquad f_n(B_n) \subset B_n'$$

が成り立つ．よって，複体写像 $f = \{f_n : C_n \longrightarrow C_n'\}$ は，

$$H(f) = \{H_n(f) : H_n(C) \longrightarrow H_n(C')\}$$

なる次数つき左 R–加群の 0 次の準同型写像をひきおこす．これを，f によりひきおこされた**ホモロジー写像**という．明らかに，$f: C \longrightarrow C'$ と $g: C' \longrightarrow C''$ が複体写像なら，$g \circ f: C \longrightarrow C''$ も複体写像で，$H(g \circ f) = H(g) \circ H(f)$ を満たす．

$(C, \partial), (C', \partial')$ を複体とし，$f, g: C \longrightarrow C'$ を複体写像とする．このとき，1 次の準同型 $s = \{s_n : C_n \longrightarrow C_{n+1}'\}$ で，

$$f_n - g_n = \partial_{n+1}' \circ s_n + s_{n-1} \circ \partial_n$$

なるものが存在するとき，$f \simeq g$ と表し，f と g は**ホモトープ**であるといい，s をその**ホモトピー**とよぶ．

$s: C \longrightarrow C'$ を f と g のホモトピーとすると，輪体 $c_n \in Z_n$ に対し，

$$\begin{aligned} f_n(c_n) - g_n(c_n) &= \partial_{n+1}'(s_n(c_n)) + s_{n-1}(\partial_n(c_n)) \\ &= \partial_{n+1}'(s_n(c_n)) \in B_n' \end{aligned}$$

が成り立つ．よって $f_n(c_n)$ と $g_n(c_n)$ は，$H_n(C') = Z_n'/B_n'$ の同じ元を定める．したがって，

命題 4.1 $f, g: C \longrightarrow C'$ がホモトープなら，$H(f) = H(g)$ となる．

一般に，複体 (C, ∂) と (C', ∂') の間に複体写像 $f: C \longrightarrow C'$ と $g: C' \longrightarrow C$ で，$g \circ f \simeq \mathrm{id}_C$，$f \circ g \simeq \mathrm{id}_{C'}$ なるものが存在するとき，(C, ∂) と (C', ∂') は**同値**であるという．このとき，命題 4.1 より，

$$H(g) \circ H(f) = \mathrm{id}_{H(C)}, \qquad H(f) \circ H(g) = \mathrm{id}_{H(C')}$$

が成り立つから，次数つき左 R–加群としての同型

$$H(C) \simeq H(C')$$

が成り立つ．

(C,∂), (C',∂'), (C'',∂'') を複体とし，

$$0 \longrightarrow C \xrightarrow{f} C' \xrightarrow{g} C'' \longrightarrow 0$$

を複体の完全列とする．つまり，f と g は複体写像で，

$$\begin{array}{ccccccccc}
 & & 0 & & 0 & & 0 & & \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
\cdots & \longrightarrow & C_{n+1} & \xrightarrow{\partial_{n+1}} & C_n & \xrightarrow{\partial_n} & C_{n-1} & \longrightarrow & \cdots \\
 & & {\scriptstyle f_{n+1}}\downarrow & & {\scriptstyle f_n}\downarrow & & {\scriptstyle f_{n-1}}\downarrow & & \\
\cdots & \longrightarrow & C_{n+1}' & \xrightarrow{\partial_{n+1}'} & C_n' & \xrightarrow{\partial_n'} & C_{n-1}' & \longrightarrow & \cdots \\
 & & {\scriptstyle g_{n+1}}\downarrow & & {\scriptstyle g_n}\downarrow & & {\scriptstyle g_{n-1}}\downarrow & & \\
\cdots & \longrightarrow & C_{n+1}'' & \xrightarrow{\partial_{n+1}''} & C_n'' & \xrightarrow{\partial_n''} & C_{n-1}'' & \longrightarrow & \cdots \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
 & & 0 & & 0 & & 0 & &
\end{array}$$

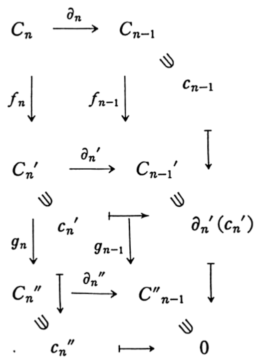
なる可換図式において，縦の列はすべて完全列をなすとする．このとき，

定理 4. 2 $$0 \longrightarrow C \xrightarrow{f} C' \xrightarrow{g} C'' \longrightarrow 0$$

が複体の完全列なら，左 R-加群の -1 次の準同型 $\partial_*: H(C'') \longrightarrow H(C)$ で，

$$\cdots \longrightarrow H_{n+1}(C'') \xrightarrow{\partial_{*,n+1}} H_n(C) \xrightarrow{H_n(f)} H_n(C') \xrightarrow{H_n(g)} H_n(C'')$$
$$\xrightarrow{\partial_{*,n}} H_{n-1}(C) \xrightarrow{H_{n-1}(f)} H_{n-1}(C') \longrightarrow \cdots$$

が完全列となるものが存在する．これを，**ホモロジー完全列**という．



[証明] $\partial_*: H(C'') \longrightarrow H(C)$ を定義するため，$c_n'' \in C_n''$ が $\partial_n''(c_n'') = 0$ を満たすとする．仮定より g_n は全射だから，$c_n' \in C_n'$ で $g_n(c_n') = c_n''$ となるものが存在する．ところが図式の可換性より，$g_{n-1}(\partial_n'(c_n')) = \partial_n''(g_n(c_n')) = 0$ だから，$\partial_n'(c_n') \in \mathrm{Ker}(g_{n-1}) = \mathrm{Im}(f_{n-1})$ となる．そこで $c_{n-1} \in C_{n-1}$ で，$f_{n-1}(c_{n-1}) = \partial_n'(c_n')$ となるものをとる．

上の手続において，c_n' を別の元 d_n' にとり替えると，$g_n(c_n' - d_n') = c_n'' - c_n'' = 0$ となる．よって $b_n \in C_n$ で，$f_n(b_n) = c_n' - d_n'$ となるものが存在する．そこで，$d_{n-1} \in C_{n-1}$ が $f_{n-1}(d_{n-1}) = \partial_n'(d_n')$ を満たすとすると，

$$f_{n-1}(c_{n-1} - d_{n-1}) = \partial_n'(c_n' - d_n') = (\partial_n' \circ f_n)(b_n) = f_{n-1}(\partial_n(b_n))$$

が成り立つ．ところが f_{n-1} は単射だから，$c_{n-1}-d_{n-1}=\partial_n(b_n)\in \mathrm{Im}(\partial_n)$ となる．よって $c_n''\in \mathrm{Ker}(\partial_n'')$ に対し，$c_{n-1}\in C_{n-1}$ の類 c_{n-1} $(\mathrm{mod}\,\mathrm{Im}(\partial_n))\in H_{n-1}(C)$ は一意的に定まる．したがって

$$\partial_{*,n}(c_n''\ (\mathrm{mod}\,\mathrm{Im}(\partial_n'')))=c_{n-1}\ (\mathrm{mod}\,\mathrm{Im}(\partial_n))$$

により，写像 $\partial_{*,n}: H_n(C'')\longrightarrow H_{n-1}(C)$ を定義できる．この $\partial_*=\{\partial_{*,n}\}: H(C'')\longrightarrow H(C)$ は，-1 次の準同型写像を与える．

定理の列の完全性は，1つずつチェックしていけば，容易にわかる．　　（証明終）

次数つき左 R-加群 $C=\bigoplus_{n\in\boldsymbol{Z}} C^n$ と，C の1次の自己準同型写像 $d=\{d^n: C^n\longrightarrow C^{n+1}\}$ の組 (C,d) で，条件

$$d^{n+1}\circ d^n=0 \qquad (\forall n\in\boldsymbol{Z})$$

を満たすものを **双対複体** という．この場合，$D_n=C^{-n}$，$\partial_n=d^{-n}$ とおくと，$D=\bigoplus_{n\in\boldsymbol{Z}} D_n$ は $\partial=\{\partial_n\}$ に関して複体となる．

(C,d) を双対複体とするとき，$\mathrm{Ker}\,d=Z(C)$ を **双対輪体加群**，$\mathrm{Im}(d)=B(C)$ を **双対境界加群** という．このとき，$Z^n(C)=\mathrm{Ker}(d^n)$ は $B^n(C)=\mathrm{Im}(d^{n-1})$ を含み，剰余加群 $H^n(C)=Z^n(C)/B^n(C)$ を，C の **コホモロジー（加）群** という．この場合にも，双対部分複体，双対複体写像，双対ホモトープ等の概念が定義できる．とくに，$0\longrightarrow C\xrightarrow{f} C'\xrightarrow{g} C''\longrightarrow 0$ が双対複体の完全列なら，準同型 $d_*{}^n: H^n(C'')\longrightarrow H^{n+1}(C)$ で

$$\cdots\longrightarrow H^{n-1}(C'')\xrightarrow{d_*{}^{n-1}} H^n(C)\xrightarrow{H^n(f)} H^n(C')\xrightarrow{H^n(g)} H^n(C'')$$
$$\xrightarrow{d_*{}^n} H^{n+1}(C)\xrightarrow{H^{n+1}(f)} H^{n+1}(C')\longrightarrow\cdots$$

を完全とするものが存在する．

4．2　射影的分解と Tor と Ext　　M を左 R-加群とする．このとき，射影的左 R-加群の列 $\{P_n\}_{0\leq n<\infty}$ と，その間の準同型の列 $\{\partial_n: P_n\longrightarrow P_{n-1}\}$ の組で，

$$\cdots\longrightarrow P_{n+1}\xrightarrow{\partial_{n+1}} P_n\xrightarrow{\partial_n} P_{n-1}\longrightarrow\cdots\longrightarrow P_1\xrightarrow{\partial_1} P_0\xrightarrow{\partial_0} M\longrightarrow 0$$

を完全列とするものを，M の **射影的分解** という．同様にして，入射的左 R-加群の列 $\{I^n\}_{0\leq n<\infty}$ と，その間の準同型の列 $\{d^n : I^n \longrightarrow I^{n+1}\}$ の組で，

$$0 \longrightarrow M \xrightarrow{d^{-1}} I^0 \xrightarrow{d^0} I^1 \xrightarrow{d^1} \cdots \longrightarrow I^{n-1} \xrightarrow{d^{n-1}} I^n \xrightarrow{d^n} I^{n+1} \longrightarrow \cdots$$

を完全列とするものを，M の **入射的分解** という．明らかに，射影的分解は複体をなし，そのホモロジーはすべて0となり，入射的分解は双対複体をなし，そのコホモロジーはすべて0となる．

定理 4.3　任意の左 R-加群 M に対し，その射影的分解は存在する．また，$P=\{P_n,\partial_n\}$ と $P'=\{P_n',\partial_n'\}$ を，各々左 R-加群 M と M' の射影的分解とし，$f: M \longrightarrow M'$ を準同型写像とする．このとき準同型写像の列 $F=\{f_n : P_n \longrightarrow P_n'\}$ で，図式

$$\begin{array}{ccccccccccc}
\cdots \longrightarrow & P_n & \xrightarrow{\partial_n} & P_{n-1} & \longrightarrow \cdots \longrightarrow & P_0 & \xrightarrow{\partial_0} & M & \longrightarrow 0 \\
& \downarrow{\scriptstyle f_n} & & \downarrow{\scriptstyle f_{n-1}} & & \downarrow{\scriptstyle f_0} & & \downarrow{\scriptstyle f} & \\
\cdots \longrightarrow & P_n' & \xrightarrow{\partial_n'} & P_{n-1}' & \longrightarrow \cdots \longrightarrow & P_0' & \xrightarrow{\partial_0'} & M' & \longrightarrow 0
\end{array}$$

を可換とするものが存在する．さらに，このような $F=\{f_n\}$ は，f を与えると，ホモトピーの差を除いて一意的に定まる．とくに，射影的分解は，同値の差を除いて，一意的に定まる．

（注）入射的分解についても，対応する定理が成り立つが，左 R-加群 M を与えたとき，M を含む入射加群 I が存在することを証明するのは，かなり面倒である．（詳しくは，彌永，小平〔B 4〕，第9章などを参照されたい．

［定理 4.3 の証明］　M を任意の左 R-加群とする．M の生成系 $\{m_i\}_{i\in I}$ をとり，$\{u_i\}_{i\in I}$ を基底とする R-自由加群を $P_0=\bigoplus_{i\in I} Ru_i$ とする．命題3.3より，R-自由加群 P_0 は射影的で，

$$\partial_0 : \quad P_0=\bigoplus_i Ru_i \ni \sum_i r_i u_i \longmapsto \sum_i r_i m_i \in M$$

は，全射な準同型写像となる．このとき，$P_0 \xrightarrow{\partial_0} M \longrightarrow 0$ は完全となるが，これを射影的分解に延長するため，$\mathrm{Ker}(\partial_0)$ を M と思い同じことを繰り返し，完全列 $P_1 \xrightarrow{\partial_1} \mathrm{Ker}(\partial_0) \longrightarrow 0$ を作る．そこでこの2つを合成すると，$P_1 \xrightarrow{\partial_1} P_0 \xrightarrow{\partial_0} M \longrightarrow 0$ なる完全列ができる．以下帰納的に，射影的左 R-加群 P_n と，完全列

$$\longrightarrow P_n \xrightarrow{\partial_n} P_{n-1} \longrightarrow \cdots \longrightarrow P_0 \xrightarrow{\partial_0} M \longrightarrow 0$$

が構成できる.

次に，P, P' を定理の通りとし，準同型写像 $f_i : P_i \longrightarrow P_i'$ $(i = 0, 1, \cdots, n-1)$ で，

$$\begin{array}{ccccccccccccc}
P_n & \xrightarrow{\partial_n} & P_{n-1} & \xrightarrow{\partial_{n-1}} & P_{n-2} & \xrightarrow{\partial_{n-2}} & \cdots & \xrightarrow{\partial_1} & P_0 & \xrightarrow{\partial_0} & M & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle f_{n-1}} & & \downarrow{\scriptstyle f_{n-2}} & & & & \downarrow{\scriptstyle f_0} & & \downarrow{\scriptstyle f} & & \\
P_n' & \xrightarrow{\partial_n'} & P_{n-1}' & \xrightarrow{\partial_{n-1}'} & P_{n-2}' & \xrightarrow{\partial_{n-2}'} & \cdots & \xrightarrow{\partial_1'} & P_0' & \xrightarrow{\partial_0'} & M' & \longrightarrow & 0
\end{array}$$

を可換とするものができたとする．このとき，$p \in \mathrm{Im}(\partial_n) = \mathrm{Ker}(\partial_{n-1})$ とすると，

$$\partial_{n-1}'(f_{n-1}(p)) = (\partial_{n-1}' \circ f_{n-1})(p) = (f_{n-2} \circ \partial_{n-1})(p) = f_{n-2}(0) = 0$$

となるから，$f_{n-1}(p) \in \mathrm{Ker}(\partial_{n-1}') = \mathrm{Im}(\partial_n')$ となる．よって，$f_{n-1} \circ \partial_n : P_n \longrightarrow \mathrm{Im}(\partial_n')$ なる準同型写像ができる．そこで準同型

$$(\partial_n')^* : \quad \mathrm{Hom}_R(P_n, P_n') \quad \longrightarrow \quad \mathrm{Hom}_R(P_n, \mathrm{Im}(\partial_n'))$$

を考える．$\partial_n' : P_n' \longrightarrow \mathrm{Im}(\partial_n')$ は全射で，P_n は射影的だから，命題 3.3 より $f_n : P_n \longrightarrow P_n'$ なる準同型写像で

$$\partial_n' \circ f_n = f_{n-1} \circ \partial_n$$

なるものが存在する．よって，帰納法により，複体写像 $F = \{f_n\} : P \longrightarrow P'$ が構成できる．

$$\begin{array}{ccccc}
P_n & & & & \\
{\scriptstyle f_n}\downarrow & & \searrow{\scriptstyle f_{n-1} \circ \partial_n} & & \\
P_n' & \xrightarrow[\partial_n']{} & \mathrm{Im}(\partial_n') & \longrightarrow & 0
\end{array}$$

次に，$F = \{f_n\}$，$F' = \{f_n'\}$ なる 2 つの複体写像が定理の条件を満たすとする．このとき $g_n = f_n - f_n'$ とおくと，これは零写像 $M \longrightarrow M'$ の延長となっている．そこで，$s_{-1} : M \longrightarrow P_0$ を零写像とし，$s_0 : P_0 \longrightarrow P_1'$，$s_1 : P_1 \longrightarrow P_2'$，…，$s_{n-1} : P_{n-1} \longrightarrow P_n'$ で

$$g_i = \partial_{i+1}' \circ s_i + s_{i-1} \circ \partial_i \qquad (0 \leqq i \leqq n-1)$$

なるものが構成できたとする．このとき，$g_{n-1} \circ \partial_n = \partial_n' \circ g_n$ だから，

$$\begin{aligned}
\partial_n' \circ (g_n - s_{n-1} \circ \partial_n) &= \partial_n' \circ g_n - \partial_n' \circ s_{n-1} \circ \partial_n = g_{n-1} \circ \partial_n - \partial_n' \circ s_{n-1} \circ \partial_n \\
&= (g_{n-1} - \partial_n' \circ s_{n-1}) \circ \partial_n = s_{n-2} \circ \partial_{n-1} \circ \partial_n = 0
\end{aligned}$$

となる．よって，$g_n - s_{n-1} \circ \partial_n$ は，$\mathrm{Ker}(\partial_n') = \mathrm{Im}(\partial_{n+1}')$ への準同型写像となる．ところが P_n は射影的で $\partial_{n+1}' : P_{n+1}' \longrightarrow \mathrm{Im}(\partial_{n+1}')$ は全射だから，命題 3.3 より，$s_n : P_n \longrightarrow P_{n+1}'$ なる準同型写像で，

$$g_n - s_{n-1} \circ \partial = \partial_{n+1}' \circ s_n$$

なるものが存在する．したがって，帰納法により，$f_n - f_n' = \partial_{n+1}' \circ s_n + s_{n-1} \circ \partial_n$ なるホモトピー $s = \{s_n : P_n \longrightarrow P_{n+1}'\}$ が構成できる．なお，このホモトピーは，$f_{-1} =$

$f_{-1}' = f$, $s_{-1} = 0$ であるから，P の最後の M を除いた複体 $\cdots \longrightarrow P_n \xrightarrow{\partial_n} P_{n-1} \longrightarrow \cdots \longrightarrow P_1 \xrightarrow{\partial_1} P_0 \longrightarrow 0$ から，P' の最後の M' を除いた複体 $\cdots \longrightarrow P_n' \xrightarrow{\partial_n'} P_{n-1}' \longrightarrow \cdots \longrightarrow P_1' \xrightarrow{\partial_1'} P_0' \longrightarrow 0$ への，複体写像 $\{f_n\}_{0 \leq n < \infty}$ と $\{f_n'\}_{0 \leq n < \infty}$ のホモトピーも与えていることに注意しておく．

最後に $M' = M$ とし，$P = \{P_n, \partial_n\}$ と $P' = \{P_n', \partial_n'\}$ が共に M の射影的分解であるとする．このとき $\mathrm{id}_M : M \longrightarrow M$ を拡張して，複体写像 $F : P \longrightarrow P'$ と $G : P' \longrightarrow P$ が作れる．しかも上で証明した一意性より，$G \circ F \simeq \mathrm{id}_P$ と $F \circ G \simeq \mathrm{id}_{P'}$ とが成り立つ．よって P と P' は同値である．なお上の注より，P と P' の最後の M を除いた複体も同値である． (証明終)

M を右 R-加群とし，N を左 R-加群とする．N の射影的分解を $P : \cdots \longrightarrow P_n \xrightarrow{\partial_n} P_{n-1} \longrightarrow \cdots \longrightarrow P_0 \xrightarrow{\partial_0} N \longrightarrow 0$ とし，P の最後の N を除いた左 R-加群の複体 $P_* : \cdots \longrightarrow P_n \xrightarrow{\partial_n} P_{n-1} \longrightarrow \cdots \longrightarrow P_1 \xrightarrow{\partial_1} P_0 \longrightarrow 0$ を作る．これは P のとり方によらず，同値の差を除き，N により一意的に定まる．そこで，この複体の $M \otimes_R$ をとり，アーベル群の列

$$M \otimes P_* : \quad \cdots \longrightarrow M \otimes_R P_n \xrightarrow{\mathrm{id} \otimes \partial_n} M \otimes_R P_{n-1} \longrightarrow \cdots \longrightarrow M \otimes_R P_1 \xrightarrow{\mathrm{id} \otimes \partial_1} M \otimes_R P_0 \longrightarrow 0$$

を作る．これは

$$(\mathrm{id} \otimes \partial_{n-1}) \circ (\mathrm{id} \otimes \partial_n) = \mathrm{id} \otimes (\partial_{n-1} \circ \partial_n) = \mathrm{id} \otimes 0 = 0$$

だから，アーベル群の複体をなす．しかも，P_* は N より（同値の差を除き）一意的に定まるから，その $M \otimes_R$ をとった $M \otimes_R P_*$ も，アーベル群の複体として，（同値の差を除き）M と N より一意的に定まる．したがって，命題 4.1 より，この複体 $M \otimes_R P_*$ のホモロジーは，M と N により（同型の差を除き）一意的に定まる．そこで

$$\mathrm{Tor}_n^R(M, N) = H_n(M \otimes_R P_*) \qquad (n \geqq 0)$$

とおき，このアーベル群を，M と N との **ねじれ積** という．

射影的分解の定義より，$P_1 \xrightarrow{\partial_1} P_0 \xrightarrow{\partial_0} N \longrightarrow 0$ は完全だから，$N \simeq P_0 / \mathrm{Im}\, \partial_1$ となる．よって $H_0(M \otimes_R P_*) = (M \otimes_R P_0)/(M \otimes_R \mathrm{Im}\, \partial_1) \simeq M \otimes_R$

$(P_0/\mathrm{Im}\,\partial_1)$ だから,

$$\mathrm{Tor}_0^R(M,N) \simeq M \otimes_R N$$

が成り立つ.

M が右 R-加群として平坦なら, $\cdots \longrightarrow P_n \xrightarrow{\partial_n} P_{n-1} \longrightarrow \cdots \longrightarrow P_0 \xrightarrow{\partial_0} N \longrightarrow 0$ の完全性より,

$$\cdots \longrightarrow M \otimes_R P_n \xrightarrow{\mathrm{id}\otimes\partial_n} M \otimes_R P_{n-1} \longrightarrow \cdots \longrightarrow M \otimes_R P_0 \xrightarrow{\mathrm{id}\otimes\partial_0} M \otimes_R N \longrightarrow 0$$

の完全性がでる. よってこの場合には,

$$\mathrm{Tor}_n^R(M,N) = \mathrm{Ker}(\mathrm{id}\otimes\partial_n)/\mathrm{Im}(\mathrm{id}\otimes\partial_{n+1}) = 0 \qquad (n \geqq 1)$$

が成り立つ.

$f: N \longrightarrow N'$ を左 R-加群の準同型写像とする. このとき $P = \{P_n, \partial_n\}$ と $P' = \{P_n', \partial_n'\}$ を N と N' の射影的分解とすると, 定理 4.3 の証明より, f は複体写像 $F = \{f_n: P_n \longrightarrow P_n'\}$ に拡張でき, しかも F の P_* への制限は, f よりホモトピーの差を除き一意的に定まる. よって, f はアーベル群の準同型写像

$$f_*: \quad \mathrm{Tor}_n^R(M,N) \longrightarrow \mathrm{Tor}_n^R(M,N')$$

を定める.

$$0 \longrightarrow N \xrightarrow{f} N' \xrightarrow{g} N'' \longrightarrow 0$$

を左 R-加群の完全列とし, $P = \{P_n, \partial_n\}$ と $P'' = \{P_n'', \partial_n''\}$ を N と N'' の射影的分解とする. このとき $P_n' = P_n \oplus P_n''$ とおくと, N' の射影的分解 $P' = \{P_n', \partial_n'\}$ と複体の短完全列 $0 \longrightarrow P \xrightarrow{F} P' \xrightarrow{G} P'' \longrightarrow 0$ で, 与えられた $0 \longrightarrow N \xrightarrow{f} N' \xrightarrow{g} N'' \longrightarrow 0$ を拡張するものが作れる (後出, 問題 4.10). したがって定理 4.2 より,

$$\cdots \longrightarrow \mathrm{Tor}_n^R(M,N) \xrightarrow{f_*} \mathrm{Tor}_n^R(M,N') \xrightarrow{g_*} \mathrm{Tor}_n^R(M,N'') \xrightarrow{\partial_*}$$

$$\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots$$

$$\xrightarrow{\partial_*} \mathrm{Tor}_1^R(M,N) \xrightarrow{f_*} \mathrm{Tor}_1^R(M,N') \xrightarrow{g_*} \mathrm{Tor}_1^R(M,N'') \xrightarrow{\partial_*}$$

$$M\otimes_R N \xrightarrow{\mathrm{id}\otimes f} M\otimes_R N' \xrightarrow{\mathrm{id}\otimes g} M\otimes_R N'' \longrightarrow 0$$

なる Tor の**完全列**ができる．とくに，左 R-加群 M が，すべての右 R-加群 N に対して

$$\mathrm{Tor}_1^R(M,N)=0$$

を満たすなら，Tor の完全系列より，M は平坦となる．

R が可換環なら，R-加群のテンソル積も R-加群となるから，$\mathrm{Tor}_n^R(M,N)$ は R-加群となり，その間の準同型 f_* などは，R-加群の準同型となる．

M, N を左 R-加群とし，M の射影的分解を　$P:\cdots\longrightarrow P_n\xrightarrow{\partial_n}P_{n-1}\longrightarrow\cdots\longrightarrow P_0\xrightarrow{\partial_0}M\longrightarrow 0$　とする．そこで

$$\mathrm{Hom}_R(P_*,N):\quad 0\longrightarrow \mathrm{Hom}_R(P_0,N)\xrightarrow{(\partial_1)^*}\mathrm{Hom}_R(P_1,N)\longrightarrow\cdots$$
$$\longrightarrow \mathrm{Hom}_R(P_{n-1},N)\xrightarrow{(\partial_n)^*}\mathrm{Hom}_R(P_n,N)\longrightarrow\cdots$$

を考える．これは　$(\partial_{n+1})^*\circ(\partial_n)^*=(\partial_n\circ\partial_{n+1})^*=0^*=0$　だから，アーベル群の双対複体をなす．また M, N を与えたとき，この双対複体は，同値の差を除き一意的に定まっている．そこでこの双対複体のコホモロジー群をとり，

$$\mathrm{Ext}_R^n(M,N)=H^n(\mathrm{Hom}_R(P_*,N))\qquad(n\geqq 0)$$

とおく．

Hom_R は左完全だから，

$$\mathrm{Ext}_R^0(M,N)=\mathrm{Ker}((\partial_1)^*)=\mathrm{Im}((\partial_0)^*)\simeq\mathrm{Hom}_R(M,N)$$

である．また M が射影的か N が入射的なら，

$$\mathrm{Ext}_R^n(M,N)=0\qquad(n\geqq 1)$$

となる．

$f:M\longrightarrow M'$ を左 R-加群の準同型とする．f は，M の射影的分解 $P=\{P_n,\partial_n\}$ から，M' の射影的分解 $P'=\{P_n',\partial_n'\}$ への複体写像に一意的に拡張できるから，コホモロジーの準同型写像

$$f^*:\quad \mathrm{Ext}_R^n(M',N)\longrightarrow\mathrm{Ext}_R^n(M,N)$$

を定める．さらに　$0\longrightarrow M\xrightarrow{f}M'\xrightarrow{g}M''\longrightarrow 0$　が左 R-加群の短完全

列なら，**Extの完全列**

$$0 \longrightarrow \mathrm{Hom}_R(M'', N) \xrightarrow{g^*} \mathrm{Hom}_R(M', N) \xrightarrow{f^*} \mathrm{Hom}_R(M, N) \xrightarrow{d^*}$$
$$\mathrm{Ext}^1_R(M'', N) \xrightarrow{g^*} \mathrm{Ext}^1_R(M', N) \xrightarrow{f^*} \mathrm{Ext}^1_R(M, N) \xrightarrow{d^*} \cdots$$

が得られる．

$$(\mathrm{E}): \quad 0 \longrightarrow N \xrightarrow{f} L \xrightarrow{g} M \longrightarrow 0$$

を左 R-加群の短完全列とする．このとき $d^*: \mathrm{Hom}_R(N, N) \longrightarrow \mathrm{Ext}^1_R(M, N)$ なる準同型が定まる．そこで $\chi(\mathrm{E}) = d^*(\mathrm{id}_N)$ とおくことにより，M の N による拡大（E）に対し，$\mathrm{Ext}^1_R(M, N)$ の元が対応する．

2つの拡大　(E)$: 0 \longrightarrow N \xrightarrow{f} L \xrightarrow{g} M \longrightarrow 0$　と　(E′)$: 0 \longrightarrow N \xrightarrow{f'} L' \xrightarrow{g'} M \longrightarrow 0$　は，

$$\begin{array}{ccccccccc} 0 & \longrightarrow & N & \xrightarrow{f} & L & \xrightarrow{g} & M & \longrightarrow & 0 \\ & & \Big\downarrow{\scriptstyle \mathrm{id}} & & \Big\downarrow{\scriptstyle \varphi} & & \Big\downarrow{\scriptstyle \mathrm{id}} & & \\ 0 & \longrightarrow & N & \longrightarrow & L' & \longrightarrow & M & \longrightarrow & 0 \end{array}$$

を可換にする同型 $\varphi: L \longrightarrow L'$ が存在するとき，**同値**であるという．このとき，M の N による拡大の同値類と $\mathrm{Ext}^1_R(M, N)$ の元とは，χ により1対1に対応することが証明できる．

4.3　2重複体　　2重次数つき左 R-加群 $C = \bigoplus_{m,n \in \mathbf{Z}} C_{m,n}$ と，その準同型写像 $\partial' = \{\partial_{m,n}' : C_{m,n} \longrightarrow C_{m-1,n}\}$，$\partial'' = \{\partial_{m,n}'' : C_{m,n} \longrightarrow C_{m,n-1}\}$ の組で，

$$\partial_{m-1,n}' \circ \partial_{m,n}' = 0, \qquad \partial_{m,n-1}'' \circ \partial_{m,n}'' = 0,$$
$$\partial_{m,n-1}' \circ \partial_{m,n}'' + \partial_{m-1,n}'' \circ \partial_{m,n}' = 0$$

を満たすものを **2重複体** という．このとき

$$C_n = \bigoplus_{p+q=n} C_{p,q}, \qquad \partial_n = \bigoplus_{p+q=n} (\partial_{p,q}' + \partial_{p,q}'')$$

とおくと，

$$\partial_{n-1} \circ \partial_n = \bigoplus_{p+q=n} \{(\partial_{p-1,q}' \circ \partial_{p,q}') + (\partial_{p,q-1}' \circ \partial_{p,q}'' + \partial_{p-1,q}'' \circ \partial_{p,q}')$$
$$+ (\partial_{p,q-1}'' \circ \partial_{p,q}'')\} = 0$$

となるから，$\{C_n, \partial_n\}$ は複体をなす．これを2重複体の **1重化** といい，そのホモロジーを $H_n(C)$ で表す．

C を2重複体とすると，任意の $q \in \boldsymbol{Z}$ に関し，$C_{*,q} = \{C_{p,q}, \partial_{p,q}{}' \ (p \in \boldsymbol{Z})\}$ は複体をなし，そのホモロジーを $H_p{}'(C_{*,q})$ で表す．このとき，条件 $\partial_{m,n-1}{}' \circ \partial_{m,n}{}'' + \partial_{m-1,n}{}'' \circ \partial_{m,n}{}' = 0$ より，$\partial_{p,q}{}''$ は $H_p{}'(C_{*,q}) \longrightarrow H_p{}'(C_{*,q-1})$ なる左 R-加群の準同型写像を定める．そこでそのホモロジーを $H_q{}''(H_p{}'(C))$ で表す．同様にして，$C_{p,*} = \{C_{p,q}, \partial_{p,q}{}''(q \in \boldsymbol{Z})\}$，$H_q{}''(C_{p,*})$，$H_p{}'(H_q{}''(C))$ などが定まる．

上で定めた2重複体の（1重化の）ホモロジー $H_n(C)$ は，このホモロジー $H_q{}''(H_p{}'(C))$ または $H_p{}'(H_q{}''(C))$ より，**スペクトル系列** の理論を使って計算できるが，その特殊な場合として，次の結果が得られる．

定理 4.4 $C = \{C_{m,n}, \partial_{m,n}{}', \partial_{m,n}{}''\}$ を2重複体とし，

$$C_{m,n} = 0 \qquad (m < 0 \text{ または } n < 0 \text{ のとき})$$

が成り立つものとする．さらに C が，

$$H_p{}'(C_{*,q}) = 0 \qquad (q \geqq 1)$$

を満たすなら，左 R-加群の同型

$$H_n(C) \simeq H_n{}'(C_{*,0}) \quad (n \geqq 0)$$

が成り立つ．

$$\begin{array}{ccccccccc}
 & & \vdots & & \vdots & & \vdots & & \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
\cdots & \longrightarrow & C_{2,2} & \longrightarrow & C_{2,1} & \longrightarrow & C_{2,0} & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
\cdots & \longrightarrow & C_{1,2} & \longrightarrow & C_{1,1} & \longrightarrow & C_{1,0} & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
\cdots & \longrightarrow & C_{0,2} & \longrightarrow & C_{0,1} & \longrightarrow & C_{0,0} & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
 & & 0 & & 0 & & 0 & &
\end{array}$$

[**証明**] 定理の仮定は，右図において，縦の列は，右端を除いてすべて完全であることを意味する．そこで，複体 $\{C_n, \partial_n\}$ のホモロジーの代表が，$C_{n,0}$ の元でとれることをいう．

$c = \sum_{p+q=n} c_{p,q} \in C_n = \bigoplus_{p+q=n} C_{p,q}$ が，$\partial_n(c) = 0$ を満たしたとする．さらに，c のホモロジー類の代表元をとり替えることにより，$0 \leqq i < n$ なる i に対し，$c_{p,q} = 0$ ($p + q = n$, $p < i$) とできたとする．このとき，仮定 $\partial_n(c) = 0$ より，

$$\begin{aligned}
\partial_{i,n-i}{}'(c_{i,n-i}) &= \partial_{i,n-i}{}'(c_{i,n-i}) + \partial_{i-1,n-i+1}{}''(c_{i-1,n-i+1}) \\
&= \partial_n(c) \text{ の } (i-1, n-i) \text{ 成分} = 0
\end{aligned}$$

が成り立つ．よって $H_p{}'(C_{*,n-i}) = 0$ だから，$d = d_{i+1,n-i} \in C_{i+1,n-i}$ で，$\partial_{i+1,n-i}{}'(d)$

$= c_{i,n-i}$ となるものが存在する．そこで $c = \sum_{p+q=n} c_{p,q}$ を，

$$c - \partial_{n+1}(d) = c - \partial_{i+1,n-i}{}'(d) - \partial_{i+1,n-i}{}''(d) = c - c_{i,n-i} - \partial_{i+1,n-i}{}''(d)$$

でおき換えると，これは c と同じホモロジー類に入り，しかも $C_{p,q}$ $(p+q=n,\ p \leqq i)$ に入る成分は 0 となる．よって帰納法で，$c_{p,q}=0$ $(p+q=n,\ p<n)$ とできる．

次に $b = \sum_{p+q=n+1} b_{p,q} \in C_{n+1} = \bigoplus_{p+q=n+1} C_{p,q}$ が，$\partial_{n+1}(b) \in C_{n,0}$ となったとする．このとき上と同様の議論で，適当に $a \in C_{n+2}$ をとり，b を $b - \partial_{n+2}(a)$ でおき換えることにより，$\partial_{n+1}(b)$ を変えずに $b_{p,q}=0$ $(p+q=n+1,\ p<n+1)$ とできることがわかる．よって

$$C_{n,0} \cap \mathrm{Im}(\partial_{n+1}) = C_{n,0} \cap \mathrm{Im}(\partial_{n+1,0}{}')$$

が成り立つ．

以上より，$H_n(C) = \mathrm{Ker}(\partial_n)/\mathrm{Im}(\partial_{n+1})$ の任意の元 h に対して，その代表元 c を　$c \in C_{n,0}$，$\partial_n(c) = \partial_{n,0}{}'(c) = 0$　となるようにとり，

$$H_n(C) \ni h \longmapsto c \ (\mathrm{mod}\ \mathrm{Im}(\partial_{n+1,0}{}')) \in H_n{}'(C_{*,0})$$

とおくと，これは左 R-加群の準同型写像で，単射となる．この写像が全射なことは明らかだから，$H_n(C) \cong H_n{}'(C_{*,0})$ が成り立つ．　　　　　　　　　　　　　（証明終）

系 4．5　2重複体 $C = \{C_{m,n}, \partial_{m,n}{}', \partial_{m,n}{}''\}$ において，$C_{m,n}=0$ $(m<0$ または $n<0)$，かつ $H_p{}'(C_{*,q})=0$ $(q \geqq 1)$，$H_q{}''(C_{p,*})=0$ $(p \geqq 1)$ が成り立つとする．このとき，左 R-加群の同型，

$$H_n{}'(C_{*,0}) \simeq H_n{}''(C_{0,*})$$

が成り立つ．

例 4．6　M を右 R-加群，N を左 R-加群とし，ねじれ積 $\mathrm{Tor}_n^R(M,N)$ を考える．

$$\cdots \longrightarrow P_m \xrightarrow{\partial_m} P_{m-1} \longrightarrow \cdots \longrightarrow P_0 \xrightarrow{\partial_0} M \longrightarrow 0$$

を M の右 R-加群としての射影的分解とし，

$$\cdots \longrightarrow Q_n \xrightarrow{\partial_n} Q_{n-1} \longrightarrow$$
$$\cdots \longrightarrow Q_0 \xrightarrow{\partial_0} N \longrightarrow 0$$

を N の左 R-加群としての射影的分解とし，これら 2 つの複体より，

$$\begin{array}{ccccccc}
 & & \vdots & & \vdots & & \vdots \\
 & & \downarrow & & \downarrow & & \downarrow \\
\cdots & \longrightarrow & P_1\otimes Q_1 & \longrightarrow & P_1\otimes Q_0 & \longrightarrow & P_1\otimes N \longrightarrow 0 \\
 & & \downarrow & & \downarrow & & \downarrow \\
\cdots & \longrightarrow & P_0\otimes Q_1 & \longrightarrow & P_0\otimes Q_0 & \longrightarrow & P_0\otimes N \longrightarrow 0 \\
 & & \downarrow & & \downarrow & & \downarrow \\
\cdots & \longrightarrow & M\otimes Q_1 & \longrightarrow & M\otimes Q_0 & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \\
 & & 0 & & 0 & &
\end{array}$$

$$C_{m,n}=\begin{cases} P_{m-1}\otimes_R Q_{n-1} & (m,n>0) \\ P_{m-1}\otimes_R N & (m>0,\ n=0) \\ M\otimes_R Q_{n-1} & (m=0,\ n>0) \\ 0 & (\text{その他}), \end{cases}$$

$\partial_{m,n}'=\partial_{m+1}\otimes\mathrm{id}$, $\partial_{m,n}''=(-1)^m\,\mathrm{id}\otimes\partial_{n+1}$ とおき，前ページ図の様なアーベル群の2重複体を作る．

ここで P_m, Q_n は射影的だから，例3.6による平担である．したがって，縦の列

$$\cdots\longrightarrow P_m\otimes_R Q_n\xrightarrow{\partial_m\otimes\mathrm{id}}P_{m-1}\otimes_R Q_n\longrightarrow\cdots\longrightarrow P_0\otimes_R Q_n\xrightarrow{\partial_0\otimes\mathrm{id}}M\otimes_R Q_n\longrightarrow 0$$

および，横の列

$$\cdots\longrightarrow P_m\otimes_R Q_n\xrightarrow{(-1)^{m+1}\otimes\partial_n}P_m\otimes_R Q_{n-1}\longrightarrow\cdots$$
$$\longrightarrow P_m\otimes_R Q_0\xrightarrow{(-1)^{m+1}\otimes\partial_0}P_m\otimes N\longrightarrow 0$$

は完全であり，この2重複体 $\{C_{m,n},\partial_{m,n}',\partial_{m,n}''\}$ は，系4.5の条件を満たす．よって

$$H_n(\{P_p\otimes_R N,\ \partial_p\otimes\mathrm{id}\})\simeq H_n(\{M\otimes_R Q_q,\ \mathrm{id}\otimes\partial_q\})$$

なるアーベル群の同型が成り立つ．

この式の右辺は，ねじれ積の定義により

$$\mathrm{Tor}_n^R(M,N)$$

に等しい．ところが，この式の左辺は，N の射影的分解を含まないから，$\mathrm{Tor}_n^R(M,N)$ が N の射影的分解のとり方によらぬことがわかる．また N が平担なら，左辺は $n\geqq 1$ のとき0となるから，

$$\mathrm{Tor}_n^R(M,N)=0 \qquad (n\geqq 1)$$

が成り立つこともわかる．

以上については，複体の2重化について述べたが，双対複体についても，2重(双対)複体が定義される．また，2重以上の多重複体も同様に定義される．

例 4.7 M, N を左 R-加群とし，$\mathrm{Ext}_R^n(M,N)$ を考える．

M の射影的分解を

$$\cdots\longrightarrow P_m\xrightarrow{\partial_m}P_{m-1}\longrightarrow\cdots\longrightarrow P_0\xrightarrow{\partial_0}M\longrightarrow 0$$

とし，N の入射的分解を

$$0\longrightarrow N\xrightarrow{d^{-1}}Q^0\xrightarrow{d^0}\cdots\longrightarrow Q^n\xrightarrow{d^n}Q^{n+1}\longrightarrow\cdots$$

とする．そこで

$$C^{m,n}=\begin{cases}\mathrm{Hom}_R(P_{m-1},Q^{n-1}) & (m,n>0)\\ \mathrm{Hom}_R(P_{m-1},N) & (m>0,\ n=0)\\ \mathrm{Hom}_R(M,Q^{n-1}) & (m=0,\ n>0)\\ 0 & (\text{その他})\end{cases}$$

とおき，右図の様な2重双対複体を作る．このとき，P_m は射影的，Q^n は入射的だから，右図において，第1行と第1列以外はすべて完全となる．よって系4.5の類似により，

$$\begin{array}{ccccccccc} & & & & 0 & & 0 & & \\ & & & & \downarrow & & \downarrow & & \\ & & 0 & \longrightarrow & C^{0,1} & \longrightarrow & C^{0,2} & \longrightarrow & \cdots \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & C^{1,0} & \longrightarrow & C^{1,1} & \longrightarrow & C^{1,2} & \longrightarrow & \cdots \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & C^{2,0} & \longrightarrow & C^{2,1} & \longrightarrow & C^{2,2} & \longrightarrow & \cdots \\ & & \downarrow & & \downarrow & & \downarrow & & \\ & & \vdots & & \vdots & & \vdots & & \end{array}$$

$$H^n(\{\mathrm{Hom}_R(P_{p+1},N),(\partial_{p+1})^*\})$$
$$\simeq H^n(\{\mathrm{Hom}_R(M,Q^q),(d^q)_*\})$$

なる左 R–加群の同型が成り立つ．この左辺は $\mathrm{Ext}_R^n(M,N)$ に等しいから，$\mathrm{Ext}_R^n(M,N)$ が M の射影的分解のとり方によらないこと，N が入射的なら

$$\mathrm{Ext}_R^n(M,N)=0 \qquad (n\geqq 1)$$

となること，$0\longrightarrow N\xrightarrow{f}N'\xrightarrow{g}N''\longrightarrow 0$ が左 R–加群の完全列なら，

$$0\longrightarrow \mathrm{Hom}_R(M,N)\xrightarrow{f_*}\mathrm{Hom}_R(M,N')\xrightarrow{g_*}\mathrm{Hom}_R(M,N'')\xrightarrow{d^*}$$
$$\mathrm{Ext}_R^1(M,N)\xrightarrow{f_*}\mathrm{Ext}_R^1(M,N')\xrightarrow{g_*}\mathrm{Ext}_R^1(M,N'')\xrightarrow{d_*}$$
$$\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots$$
$$\xrightarrow{d^*}\mathrm{Ext}_R^n(M,N)\xrightarrow{f_*}\mathrm{Ext}_R^n(M,N')\xrightarrow{g_*}\mathrm{Ext}_R^n(M,N'')\xrightarrow{d^*}\cdots$$

なる Ext の**完全列**ができることなどがわかる．

以上では，テンソル積 $M\otimes_R N$ より $\mathrm{Tor}_n^R(M,N)$ を作る方法と，$\mathrm{Hom}_R(M,N)$ より $\mathrm{Ext}_R^n(M,N)$ を作る方法のみのべたが，これらの方法を多少一般化すれば，より一般の関手に対しても，その**導来関手**を作ることができる(彌永，小平〔B 4〕，第9章などを参照)．

例 4.8 G を群とする．このとき，R を記号 u_σ $(\sigma\in G)$ 全体で生成される $\boldsymbol{Z}$–自由加群とし，R における積を，

$$\Big(\sum_{\sigma\in G}a_\sigma u_\sigma\Big)\cdot\Big(\sum_{\sigma\in G}b_\sigma u_\sigma\Big)=\sum_{\sigma,\tau\in G}a_\sigma b_\tau u_{\sigma\tau}$$

$(a_\sigma, b_\sigma \in \boldsymbol{Z})$ で定義する．このとき R は多元環となる．これを G の **群環** とよび，$\boldsymbol{Z}[G]$ で表す．

整数 $n \geqq 0$ に対し，

$$P_n = R \otimes_{\boldsymbol{Z}} R \otimes_{\boldsymbol{Z}} \cdots \otimes_{\boldsymbol{Z}} R \qquad (n+1 \text{ 個のテンソル積})$$

とおく．これは左 R-加群としては，

$$[\sigma_1, \sigma_2, \cdots, \sigma_n] = 1 \otimes \sigma_1 \otimes \sigma_2 \otimes \cdots \otimes \sigma_n \qquad (\sigma_1, \sigma_2, \cdots, \sigma_n \in G)$$

全体を基底とする R-自由加群となる．そこで，$n > 0$ のとき，

$$\partial_n[\sigma_1, \sigma_2, \cdots, \sigma_n] = \sigma_1[\sigma_2, \cdots, \sigma_n] + \sum_{1 \leq i \leq n-1} (-1)^i [\sigma_1, \sigma_2, \cdots, \sigma_i \cdot \sigma_{i+1}, \cdots, \sigma_n] + (-1)^n [\sigma_1, \sigma_2, \cdots, \sigma_{n-1}]$$

とおき，左 R-加群の準同型写像

$$\partial_n: \quad P_n \longrightarrow P_{n-1}$$

を定義する．

$\varepsilon: R = \boldsymbol{Z}[G] \longrightarrow \boldsymbol{Z}$ なる $\boldsymbol{Z}$-加群の準同型写像を

$$\varepsilon\Bigl(\sum_{\sigma \in G} a_\sigma u_\sigma\Bigr) = \sum_{\sigma \in G} a_\sigma \qquad (a_\sigma \in \boldsymbol{Z})$$

で定義する．このとき $\boldsymbol{Z}$ は，$r \cdot n = \varepsilon(r) \cdot n$ $(r \in R,\ n \in \boldsymbol{Z})$ なる作用で，左 R-加群と思える．さらに $P_0 = R$ だから，$\partial_0 = \varepsilon$ とおくと，$\partial_0: P_0 \longrightarrow \boldsymbol{Z}$ は，左 R-加群の準同型写像となる．そこで

$$\cdots \longrightarrow P_n \xrightarrow{\partial_n} P_{n-1} \longrightarrow \cdots \longrightarrow P_0 \xrightarrow{\partial_0} \boldsymbol{Z} \longrightarrow 0$$

なる左 R-加群の列を考える．これらは，$\partial_{n-1} \circ \partial_n = 0$ を満たし，左 R-加群の複体をなす．また

$$\eta: \quad \boldsymbol{Z} \ni n \longmapsto n u_1 \in R$$

とおき，$s_n: P_n \longrightarrow P_{n+1}$ を

$$s_n(\sigma_0[\sigma_1, \sigma_2, \cdots, \sigma_n]) = [\sigma_0, \sigma_1, \sigma_2, \cdots, \sigma_n]$$

で定義する．とくに $s_{-1} = \eta: \boldsymbol{Z} \longrightarrow R = P_0$ とおく．このとき

$$\partial_{n+1} \circ s_n + s_{n-1} \circ \partial_n = \mathrm{id}_{P_n} \qquad (n \geqq 0)$$

が成り立つ．よって $p \in P_n$ が $\partial_n(p) = 0$ を満たすなら，$p = \partial_{n+1}(s_n(p))$ と書ける．したがって，上の複体は完全列をなしている．

P_n は R-自由加群だから射影的である．よって，上の複体は，$\boldsymbol{Z}[G]$-加群 $\boldsymbol{Z}$ の射影的分解を与える．

A を任意の左 R-加群とする．このとき，A に係数をもつ **群 G のホモロジー群** $H_n(G,$

$A)$ と **コホモロジー群** $H^n(G, A)$ を，

$$H_n(G, A) = \mathrm{Tor}_n^{\boldsymbol{Z}[G]}(\boldsymbol{Z}, A), \qquad H^n(G, A) = \mathrm{Ext}^n_{\boldsymbol{Z}[G]}(\boldsymbol{Z}, A)$$

で定義する．これらは，上で定義した $\boldsymbol{Z}$ の標準的分解を通して，次の様に計算できる．

簡単のため，コホモロジーのみを計算する．P_n は射影的だから，

$$0 \longrightarrow \mathrm{Hom}_{\boldsymbol{Z}[G]}(\boldsymbol{Z}, A) \xrightarrow{\partial_0^*} \mathrm{Hom}_{\boldsymbol{Z}[G]}(P_0, A) \longrightarrow \cdots$$
$$\longrightarrow \mathrm{Hom}_{\boldsymbol{Z}[G]}(P_{n-1}, A) \xrightarrow{\partial_n^*} \mathrm{Hom}_{\boldsymbol{Z}[G]}(P_n, A) \longrightarrow \cdots$$

が複体をなし，そのホモロジーが $H^n(G, A)$ をなす．P_n は $1 \otimes \sigma_1 \otimes \sigma_2 \otimes \cdots \otimes \sigma_n = [\sigma_1, \sigma_2, \cdots, \sigma_n]$ を基底とする $\boldsymbol{Z}[G]$-自由加群だから，

$$\mathrm{Hom}_{\boldsymbol{Z}[G]}(P_n, A) = \{f : G^n \longrightarrow A\}$$

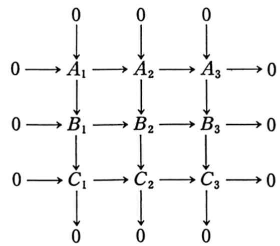
とみなせる．このとき $\delta^n = \partial_n^*$ は，

$$(\delta^n f)(\sigma_1, \sigma_2, \cdots, \sigma_{n+1}) = \sigma_1 f(\sigma_2, \cdots, \sigma_{n+1})$$
$$+ \sum_{1 \le i \le n} (-1)^i f(\sigma_1, \cdots, \sigma_i \cdot \sigma_{i+1}, \cdots, \sigma_{n+1}) + (-1)^{n+1} f(\sigma_1, \cdots, \sigma_n)$$

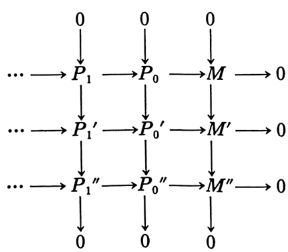
となる．とくに

$$(\delta^0 f)(\sigma) = \sigma f - f$$
$$(\delta^1 f)(\sigma, \tau) = \sigma f(\tau) - f(\sigma\tau) + f(\sigma)$$
$$(\delta^2 f)(\sigma, \tau, \rho) = \sigma f(\tau, \rho) - f(\sigma\tau, \rho) + f(\sigma, \tau\rho) + f(\sigma, \tau)$$

が成り立つ．



問題 4.9　(3 × 3 - lemma)　右上の図の様な左 R-加群の可換図式において，縦の列はすべて完全で，横の列も上2つまたは下2つの列は完全であるとする．このとき，残りの列も完全となることを示せ．



問題 4.10　$0 \longrightarrow M \xrightarrow{f} M' \xrightarrow{g} M'' \longrightarrow 0$ を左 R-加群の完全列とする．このとき M, M', M'' の射影的分解 P, P', P'' と，f, g の複体写像への拡張 F, G で，

$$0 \longrightarrow P \xrightarrow{F} P' \xrightarrow{G} P'' \longrightarrow 0$$

が完全となるものが存在することを示せ．

§5.　単因子の理論と行列の標準化

この§では，加群の例として単項イデアル整域上の有限生成の加群の性質を調べ，それを使って行列の標準型を導く．この§の結果は，以後では使わない．

5.1　単因子論　R を単項イデアル整域とする．このとき第Ⅲ章，定理4.4により，R は一意分解環となる．したがって，約数，倍数，素元，同伴などの言葉を，第Ⅲ章，§4の意味で使う．

5.1では，次の2つの定理を証明する．

定理5.1　R を単項イデアル整域，F を階数 n の R-自由加群，N を F の R-部分加群とする．このとき，F の基底 $\{u_1, u_2, \cdots, u_n\}$ と R の元 $e_1, e_2, \cdots, e_r$ $(r \leqq n,\ e_i \neq 0)$ で，

$$N = Re_1u_1 + Re_2u_2 + \cdots + Re_ru_r, \qquad e_i | e_{i+1} \qquad (i = 1, 2, \cdots, r-1)$$

となるものが存在する．しかも，R のイデアルの集合 $\{(e_1), (e_2), \cdots, (e_r)\}$ は，F の基底のとり方によらず，F と N より一意的に定まる．

定理5.2　R を単項イデアル整域，M を有限生成 R-加群とする．このとき，R の0でも単数でもない元 $e_1, e_2, \cdots, e_r$ で，

$$M \simeq R/(e_1) \oplus R/(e_2) \oplus \cdots \oplus R/(e_r) \oplus \underbrace{R \oplus R \oplus \cdots \oplus R}_{s\text{個}}$$
$$e_i | e_{i+1} \qquad (1 \leqq i \leqq r-1)$$

となるものが存在する．しかも，R のイデアルの集合 $\{(e_1), (e_2), \cdots, (e_r), 0, \cdots, 0\ (s\text{個の}\ 0)\}$ は，上の様な直和分解の仕方によらず，M の同型類により一意的に定まる．これを M の**不変系**という．

［2つの定理の関係］　M を有限生成 R-加群とし，その生成系を $\{v_1, v_2, \cdots, v_n\}$ とし，$F = R \oplus R \oplus \cdots \oplus R$ を階数 n の R-自由加群とする．このとき，R-加群の準同型写像

$$f:\quad F \ni (r_1, r_2, \cdots, r_n) \longmapsto \sum_{1 \leqq i \leqq n} r_i v_i \in M$$

は全射となる．そこで，$N=\mathrm{Ker}(f)$ とおくと，$M\simeq F/N$ であるから，定理 5.1 の前半より定理 5.2 の前半が導かれる．ここで，e_i が単数のときは，$R/(e_i)=0$ だから，定理 5.2 ではこのようなものは除いた．また F, N を定理 5.1 の通りとすると，$M=F/N$ は，定理 5.2 の形となる．よって，定理 5.2 の後半より，定理 5.1 の後半が導かれる．したがって，定理 5.1 の前半と定理 5.2 の後半を示せばよい．

まず補題を 2 つ用意する．

補題 5.3　R を可換環とし，F を有限生成の R-自由加群とする．このとき F の基底 $\{u_1, u_2, \cdots, u_n\}$ の個数 n は，基底のとり方によらず一定である．これを $\mathrm{rank}_R\, F$ と表す．

[証明]　$\mathfrak{m}$ を R の極大イデアルとする．このとき，$F\simeq R\oplus R\oplus\cdots\oplus R$ (n 個の和) だから，問題 2.7 より，

$$F\otimes_R (R/\mathfrak{m})\simeq (R/\mathfrak{m})\oplus(R/\mathfrak{m})\oplus\cdots\oplus(R/\mathfrak{m}) \qquad (n\text{ 個の和})$$

となる．ところが例 1.3 より，体 $R/\mathfrak{m}$ 上のベクトル空間の次元として，n は F (と $\mathfrak{m}$) により一意的に定まっている．　(証明終)

補題 5.4　R を単項イデアル整域，W を $\{w_1, w_2\}$ を基底にもつ階数 2 の R-自由加群，$w=r_1w_1+r_2w_2$ $(0\neq r_1, r_2\in R)$ を W の元とする．このとき d を r_1, r_2 の最大公約数とすると，W の基底 $\{w_1', w_2'\}$ で，$w=dw_1'$ となるものが存在する．

[証明]　$r_1=ds_1$, $r_2=ds_2$ $(s_1, s_2\in R)$ とおく．s_1, s_2 は仮定より互いに素だから，

$\det\begin{pmatrix} s_1 & s_2 \\ t_1 & t_2 \end{pmatrix}=t_2s_1-t_1s_2=1$　となる $t_1, t_2\in R$ が存在する．そこで

$$w_1'=s_1w_1+s_2w_2, \qquad w_2'=t_1w_1+t_2w_2$$

とおくと，t_1, t_2 のとり方より，

$$w_1=t_2w_1'-s_2w_2', \qquad w_2=-t_1w_1'+s_1w_2'$$

と書ける．よって $\{w_1', w_2'\}$ も W の基底で，

$$\begin{aligned} w &= r_1(t_2w_1'-s_2w_2')+r_2(-t_1w_1'+s_1w_2') \\ &= d(s_1t_2-s_2t_1)w_1'+d(-s_1s_2+s_2s_1)w_2'=dw_1' \end{aligned}$$

となる．　(証明終)

[定理 5.1 の存在の証明]　F, Nを定理の通りとする．$n = \mathrm{rank}_R F$が1のときは，$F \simeq R$なる同型で，NにはRのイデアル$\mathfrak{a}$が対応する．ところがRは単項イデアル整域だから，$\mathfrak{a} = (e_1)$（$\exists e_1 \in R$）と書ける．よってFの基底を$\{u_1\}$とすると，$N = Re_1u_1$となり，定理が成り立つ．したがって，$n \geqq 2$とし，帰納法により，階数がnより小のときは，求めるような基底が存在すると仮定する．

$B = \{v_1, v_2, \cdots, v_n\}$を$F$の基底とし，$N$の元$m = \sum_{1 \leqq i \leqq n} r_i v_i$（$r_i \in R$）を動かす．このとき$r_1 \in R$の全体は，$R$のイデアル$\mathfrak{a}(B)$をなす．ここで$B$を動かし，集合$\{\mathfrak{a}(B)\}$を作る．これはネター環$R$のイデアルの集合だから，極大元が存在する．よって$B = \{v_1, v_2, \cdots, v_n\}$のとき，$\mathfrak{a}(B)$が極大となるものとする．$\mathfrak{a}(B)$は単項イデアル環$R$のイデアルであるから，$\mathfrak{a}(B) = (e_1)$（$\exists e_1 \in R$）と書ける．このとき$\mathfrak{a}(B)$の定義より，

$$m = e_1v_1 + r_2v_2 + \cdots + r_nv_n \qquad (r_i \in R)$$

の形のNの元mが存在する．

$W = Rv_1 \oplus Rv_2$，$w = e_1v_1 + r_2v_2$　とし，dをe_1とr_2の最大公約数とする．そこで$W \ni w$に補題 5.4 を使い，Wの基底$\{v_1', v_2'\}$で，$w = dv_1'$となるものを作る．このとき，$\{v_1', v_2', v_3, \cdots, v_n\}$は$F$の基底であり，$m = dv_1' + *v_2' + *v_3 + \cdots \in N$，$(e_1) \subset (d)$となる．よって$\mathfrak{a}(B) = (e_1)$の極大性より，$(d) = (e_1)$となり，$e_1 | r_2$が成り立つ．同様にして，$e_1 | r_i$ $(i \geqq 2)$も成り立つ．よって$r_i = e_1 r_i'$，$u_1 = v_1 + r_2'v_2 + \cdots + r_n'v_n$とおくと，$\{u_1, v_2, \cdots, v_n\}$は$F$の基底で，$m = e_1u_1$と書ける．

$F' = Rv_2 + \cdots + Rv_n \subset F$　とおく．これは階数$n-1$のR-自由加群である．そこで，

$$f: \quad N \ni t_1u_1 + t_2v_2 + \cdots + t_nv_n \longmapsto t_1 \in R$$

で定義されるR-加群の準同型写像を考える．明らかに，$\mathrm{Ker}(f) = N \cap F'$である．また$\mathrm{Im}(f) \supset (e_1)$であるが，$\mathrm{Im}(f)$は$R$のイデアルだから単項イデアルとなり，$N$の元　$t_1u_1 + t_2v_2 + \cdots + t_nv_n$　で$\mathrm{Im}(f) = (t_1)$となるものが存在する．ところが$\mathfrak{a}(B) = (e_1)$は極大にとったから，$\mathrm{Im}(f) = (t_1) = (e_1)$が成り立つ．

$\mathrm{Im}(f) = e_1R$はR-自由加群だから，命題 3.3 より，$0 \longrightarrow \mathrm{Ker}(f) \longrightarrow N \longrightarrow \mathrm{Im}(f) \longrightarrow 0$　なる短完全列は分解する．よって，R-加群Nは，

$$N = Re_1u_1 \oplus (N \cap F')$$

と直和に分解する．そこで　$F' = Rv_2 \oplus \cdots \oplus Rv_n \supset N' = N \cap F'$　に対し帰納法の

仮定を使い，F' の基底 $\{u_2, \cdots, u_n\}$ と R の元 $e_2, \cdots, e_r$ で，$N \cap F' = Re_2u_2 + \cdots + Re_r u_r$，$e_i | e_{i+1}$ $(2 \leqq i \leqq r-1)$ なるものを作る．このとき $N \ni e_1u_1 + e_2u_2$ であるから，(e_1) の極大性と補題5.4より $e_1|e_2$ となる．　(証明終)

定理5.2の一意性を示すため，定理5.2を次の形に変形しておく．

定理5.5　M を単項イデアル整域 R 上の有限生成 R-加群とする．このとき，R の素元の集合 $p_1, p_2, \cdots, p_k$ と，自然数の増加列 $n_{i,1} \leqq n_{i,2} \leqq \cdots \leqq n_{i,r(i)}$ で，

$$M \simeq (\bigoplus_{1 \leq i \leq k} \bigoplus_{1 \leq j \leq r(i)} R/(p_i^{n_{i,j}})) \oplus R^s$$

となるものが存在する．しかも，ここにでてくるイデアルの集合 $\{(p_i^{n_{i,j}}) | 1 \leqq i \leqq k,\ 1 \leqq j \leqq r(i)\}$ と s は，上のような直和分解の仕方によらず，M の同型類により一意的に定まる．

[定理5.2と5.5の関係]　M を定理5.5の通りとすると，定理5.2より

$$M \simeq (\bigoplus_{1 \leq j \leq r} R/(e_j)) \oplus R^s, \qquad e_j | e_{j+1} \qquad (1 \leqq j \leqq r-1)$$

と書ける．ここで，R の素元全体を同伴という関係で分類し，その完全代表系 P をとる．R は一意分解環だから，R の元 e_j $(j = 1, 2, \cdots, r)$ は

$$e_j = u_j \prod_i p_i^{n_{i,j}} \qquad (u_j \text{ は } R \text{ の単数，} p_i \in P,\ 0 \leqq n_{i,j} \in \boldsymbol{Z})$$

の形に一意的に書ける．ここで各 p_i は互いに素だから，$(p_i^{n_{i,j}}) + (p_k^{n_{k,j}}) = R$ $(i \neq k)$ が成り立つ．よって，第Ⅲ章，命題1.8により，

$$R/(e_j) \simeq \bigoplus_i R/(p_i^{n_{i,j}})$$

と書ける．これを $(\bigoplus_{1 \leq j \leq r} R/(e_j)) \oplus R^s$ に代入して整理すると，定理5.5の前半を得る．また，定理5.5の一意性から，定理5.2の一意性が従うことも，R が一意分解環だから，以上の議論よりわかる．

[定理5.5の一意性の証明]　R を整域とし，M を R-加群とする．このとき，M のねじれ元全体を，

$$t(M) = \{m \in M \mid 0 \neq \exists r \in R \text{ に対し } rm = 0\}$$

とおくと，$t(M)$ は M の R-部分加群となり，$M/t(M)$ はねじれ元をもたない (1.1参照)．

$$M \simeq (\bigoplus_i \bigoplus_j R/(p_i^{n_{i,j}})) \oplus R^s$$

を定理の通りとする．このとき $t(M) \simeq \bigoplus_i \bigoplus_j R/(p_i^{n_{i,j}})$ となる．よって $M/t(M) \simeq R^s$ となる．したがって，補題5.3より，R-自由加群 $M/t(M)$ の階数として，s は一意的に定まる．よって

$$M \simeq \bigoplus_{1 \leq i \leq k} \bigoplus_{1 \leq j \leq r(i)} R/(p_i^{n_{i,j}}) \qquad (n_{i,1} \leqq n_{i,2} \leqq \cdots \leqq n_{i,r(i)})$$

として，一意性を示せばよい．

p_i と p_k $(i \neq k)$ は互いに素だから，$(p_i^{n_{i,r(i)}}) + (p_k^{n_{k,j}}) = R$ となる． よって $q_i = p_i^{n_{i,r(i)}}$ は，$R/(p_k^{n_{k,j}})$ の上に単数として作用する．したがって，

$$f_i: \quad M \ni m \longmapsto q_i m \in M$$

により，M の自己準同型写像を定義すると，

$$\mathrm{Ker}(f_i) \simeq \bigoplus_{1 \leq j \leq r(i)} R/(p_i^{n_{i,j}})$$

となる．これは M （と q_i） より定まる．よって

$$M \simeq R/(p^{n_1}) \oplus R/(p^{n_2}) \oplus \cdots \oplus R/(p^{n_r})$$

（p は R の素元，$n_1 \leqq n_2 \leqq \cdots \leqq n_r$） として，$\{n_1, n_2, \cdots, n_r\}$ の一意性をいえばよい．

この場合，n_r は

$$\min\{n \mid n \in \boldsymbol{N},\ p^{n-1}M \neq \{0\},\ p^n M = \{0\}\}$$

として，M によって一意的に定まっている．そこで $n(M) = n_r$ とおき，$n(M)$ に関する帰納法で一意性を示す．

$$pM \simeq pR/(p^{n_1}) \oplus pR/(p^{n_2}) \oplus \cdots \oplus pR/(p^{n_r}) = \bigoplus_{1 \leq j \leq r,\ 2 \leq n_j} R/(p^{n_j - 1}),$$

$$M/pM \simeq R/(p) \oplus R/(p) \oplus \cdots \oplus R/(p) \qquad (r \text{ 個の直和})$$

である．ところが $R/(p)$ は体だから，r はベクトル空間 M/pM の次元として，M より一意的に定まる（例1.3参照）．とくに，$n(M) = 1$ なら，$pM = \{0\}$，$n_1 = n_2 = \cdots = n_r = 1$ となるから，$\{n_1, n_2, \cdots, n_r\}$ は M より一意的に定まる． 一般に，$n(pM) = n(M) - 1$ だから，帰納法の仮定を pM に使うと，$\{n_j - 1 \mid 1 \leqq j \leqq r,\ 2 \leqq n_j\}$ が M より一意的に定まっていることがわかる．よって，r とこの集合の元の個数の差として，$\#\{n_j \mid 1 \leqq j \leqq r,\ n_j = 1\}$ も定まり，$\{n_1, n_2, \cdots, n_r\}$ が M により一意的に定まっていることがわかる． （証明終）

例 5.6 （アーベル群の基本定理） $R = \boldsymbol{Z}$ とする．このとき定理5.5より，任意の有限生成アーベル群 G は，

$$G \simeq (\bigoplus_{1 \leq i \leq k} \bigoplus_{1 \leq j \leq r(i)} \boldsymbol{Z}/p_i^{n_{i,j}}\boldsymbol{Z}) \oplus \boldsymbol{Z}^s$$

($p_1, p_2, \cdots, p_k$ は相異なる素数，$1 \leqq n_{i,1} \leqq n_{i,2} \leqq \cdots \leqq n_{i,r(i)}$) と巡回群の直和の形に書け，しかも，$s$ と $\{p_i^{n_{i,j}} \mid 1 \leqq i \leqq k,\ 1 \leqq j \leqq r(i)\}$ は G により一意的に定まっていることがわかる．これは，第Ⅱ章，定理 6.1 の一般化を与える．

問 題 5. 7　R を単項イデアル整域，M を有限生成 R-加群とする．このとき，（1）M はねじれがない，（2）M は射影的である，（3）M は自由加群である，の 3 つは互いに同値であることを示せ．

5. 2　行列の標準化 I

R を可換環とし，R を R 自身の上に乗法で作用させ R-加群と思う（第Ⅰ章，例 7.3 参照）．このとき自然数 n に対し，R^n で R の n 個の直和のなす R-加群を表すと，R^n は

$$\boldsymbol{x} = \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix} \qquad (x_1, x_2, \cdots, x_n \in R)$$

の形の縦ベクトル全体のなす集合と思える．ここで，$r \in R$ は R^n に，

$$r \cdot \boldsymbol{x} = r \cdot {}^t(x_1, x_2, \cdots, x_n) = {}^t(r \cdot x_1,\ r \cdot x_2,\ \cdots,\ r \cdot x_n)$$

の形で作用するものとする（第Ⅰ章，§10参照）．以下簡単のため，R-加群の間の準同型写像を，**線型写像** とよぶ．

$f : R^n \longrightarrow R^m$ を線型写像とする．このとき，f による R^n の標準的な基底

$$\boldsymbol{e}_1 = \begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}, \quad \boldsymbol{e}_2 = \begin{pmatrix} 0 \\ 1 \\ \vdots \\ 0 \end{pmatrix}, \quad \cdots, \quad \boldsymbol{e}_n = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 1 \end{pmatrix}$$

のゆき先を

$$f(\boldsymbol{e}_1) = \begin{pmatrix} a_{11} \\ a_{21} \\ \vdots \\ a_{m1} \end{pmatrix}, \quad f(\boldsymbol{e}_2) = \begin{pmatrix} a_{12} \\ a_{22} \\ \vdots \\ a_{m2} \end{pmatrix}, \quad \cdots, \quad f(\boldsymbol{e}_n) = \begin{pmatrix} a_{1n} \\ a_{2n} \\ \vdots \\ a_{mn} \end{pmatrix}$$

と表し,

$$A = \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \cdots & \cdots & \cdots & \cdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{pmatrix} \in M(m, n; R)$$

とおく．このとき線型写像 $f : R^n \longrightarrow R^m$ は，行列の乗法

$$R^n \ni \boldsymbol{x} \longmapsto A \cdot \boldsymbol{x} \in R^m \qquad (\boldsymbol{x} = {}^t(x_1, x_2, \cdots, x_n))$$

によって表される．

次に，線型写像 $g : R^n \longrightarrow R^m$ が，上と同じ意味で行列 $B = (b_{ij}) \in M(m, n ; R)$ により表されたとする．このとき，

$$(f+g)(\boldsymbol{x}) = f(\boldsymbol{x}) + g(\boldsymbol{x}) = A \cdot \boldsymbol{x} + B \cdot \boldsymbol{x} = (A+B) \cdot \boldsymbol{x} \qquad (\boldsymbol{x} \in R^n)$$

が成り立つ．よって，写像の和 $f+g$ には行列の和 $A+B$ が対応するから，

$$\iota : \quad \mathrm{Hom}_R(R^n, R^m) \ni f \quad \longmapsto \quad A \in M(m, n ; R) \qquad (f(\boldsymbol{x}) = A \cdot \boldsymbol{x})$$

は群の準同型写像を与える．

R は可換環だから，$\mathrm{Hom}_R(R^n, R^m)$ は $(r \cdot f)(\boldsymbol{x}) = r \cdot f(\boldsymbol{x})$ とおくことにより R–加群となっている (1.1 参照)．他方 $M(m, n ; R)$ も $r \cdot (a_{ij}) = (r \cdot a_{ij})$ なる作用で R–加群となっている (第 I 章，§10 参照)．しかも上の対応 $\iota : f \longmapsto A$ は，この R の作用を保つから，R–加群の準同型写像となる．

この写像 ι は，$f(\boldsymbol{x}) = A \cdot \boldsymbol{x}$ なる関係より，明らかに単射である．また任意の $A \in M(m, n ; R)$ に対し，$f(\boldsymbol{x}) = A \cdot \boldsymbol{x}$ で f を定めると，f は $\mathrm{Hom}_R(R^n, R^m)$ の元で，上の対応で A が対応する．よって上の対応は R–加群の同型である．

$h : R^m \longrightarrow R^l$ が，前と同じ意味で $C = (c_{hi}) \in M(l, m ; R)$ で表されたとする．このとき，

$$(h \circ f)(\boldsymbol{x}) = h(f(\boldsymbol{x})) = h(A \cdot \boldsymbol{x}) = C \cdot (A \cdot \boldsymbol{x}) = (C \cdot A)(\boldsymbol{x}) \qquad (\boldsymbol{x} \in R^n)$$

が成り立つ．よって上の対応 $f \longmapsto A$ により，写像の合成には対応する行列の積が対応する．

とくに $m=n$ とすると，

$$\iota:\quad \mathrm{End}_R(R^n)\ni f \longmapsto A\in M_n(R) \qquad (f(\boldsymbol{x})=A\cdot\boldsymbol{x})$$

なる対応は，環の同型を与えることがわかる．ところが $A\in M_n(R)$ が単数となる必要十分条件は，第 I 章，定理 10.5 より $\det(A)$ が R の単数となることである．よって $f\in \mathrm{End}_R(R^n)$ が同型となるための必要十分条件は，f を表す行列が

$$GL_n(R)=\{A\in M_n(R)\mid \det(A)\ \text{は}\ R\ \text{の単数}\}$$

なる群に入ることである．よって，次の命題を得る．

命題 5.8　R を可換環とし，R^n を R 上長さ n の縦ベクトル全体のなす R–加群とする．このとき，

（1）　$f:R^n\longrightarrow R^m$ なる任意の線型写像 f は，適当な行列 $A\in M(m,n;R)$ をとると，

$$f(\boldsymbol{x})=A\cdot\boldsymbol{x} \qquad (\boldsymbol{x}\in R^n)$$

の形で与えられる．

（2）（1）で定めた対応 $f\longmapsto A$ は，

$$\mathrm{Hom}_R(R^n,R^m)\simeq M(m,n;R)$$

なる R–加群の同型をひきおこす．また，$m=n$ のときは，

$$\mathrm{End}_R(R^n)\simeq M_n(R)$$

なる環の同型と，

$$\mathrm{Aut}_R(R^n)\simeq GL_n(R)$$

なる群の同型をひきおこす．

以上の準備のもとで，次の定理を証明する．

定理 5.9　R を単項イデアル整域，$A\in M(m,n;R)$ を R 上の $m\times n$ 行列とする．このとき $P\in GL_m(R)$ と $Q\in GL_n(R)$ を適当にとると，

$$PAQ = \left(\begin{array}{cccc|c} e_1 & & & 0 & \\ & e_2 & & & 0 \\ & & \ddots & & \\ 0 & & & e_r & \\ \hline & & 0 & & 0 \end{array}\right), \qquad 0 \neq e_i \in R,\ e_i | e_{i+1} \quad (1 \leqq i \leqq r-1)$$

と書ける．ここで，R のイデアルの集合 $\{(e_1), (e_2), \cdots, (e_r)\}$ は P, Q のとり方によらず，A により一意的に定まる．これを A の **単因子** という．

[証 明] R^m, R^n を，各々 R 上の長さ m, n の縦ベクトル全体のなす R-加群とし，$A = (a_{ij})$ $(1 \leqq i \leqq m,\ 1 \leqq j \leqq n)$ とおく．このとき A は，

$$R^n \ni \boldsymbol{x} \longmapsto A \cdot \boldsymbol{x} \in R^m$$

により，線型写像 $f: R^n \longrightarrow R^m$ を定める．

R^m は階数 m の R-自由加群で，$\mathrm{Im}(f)$ は R^m の R-部分加群だから，定理 5.1 より，R^m の適当な基底 $\{u_1, u_2, \cdots, u_m\}$ をとると，

$$\mathrm{Im}(f) = Re_1u_1 \oplus Re_2u_2 \oplus \cdots \oplus Re_ru_r \qquad (r \leqq m,\ 0 \neq e_i \in R,\ e_i | e_{i+1})$$

と書ける．しかも，$\{(e_1), (e_2), \cdots, (e_r)\}$ は $\mathrm{Im}(f)$ により一意的に定まる．

$\mathrm{Im}(f)$ は R-自由加群だから，命題 3.3 より，

$$0 \longrightarrow \mathrm{Ker}(f) \longrightarrow R^n \xrightarrow{f} \mathrm{Im}(f) \longrightarrow 0$$

なる短完全列は分解する．よって，R^n の R-部分加群 V で，f は $V \xrightarrow{\sim} \mathrm{Im}(f)$ なる同型をひきおこし，

$$R^n = V \oplus \mathrm{Ker}(f)$$

となるものが存在する．そこで $\{v_1, v_2, \cdots, v_r\}$ を V の基底で，$f(v_i) = e_iu_i$ となるものをとる．

$\mathrm{Ker}(f)$ は，R-自由加群 R^n の R-部分加群であるから，定理 5.1 より R-自由加群である．そこで $\{v_{r+1}, v_{r+2}, \cdots, v_n\}$ を $\mathrm{Ker}(f)$ の基底とすると，$\{v_1, v_2, \cdots, v_r, v_{r+1}, v_{r+2}, \cdots, v_n\}$ は R^n の基底となる．$v_j \in R^n$ を縦ベクトルとして

$$v_j = {}^t(v_{1j}, v_{2j}, \cdots, v_{nj}) \qquad (v_{1j}, v_{2j}, \cdots, v_{nj} \in R)$$

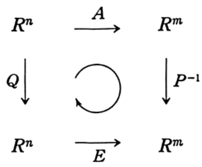
と表現し，

$$Q = (v_{ij}) \qquad (1 \leqq i, j \leqq n)$$

とおく．このとき Q なる行列は，R^n の基底を $\{\boldsymbol{e}_1, \boldsymbol{e}_2, \cdots, \boldsymbol{e}_n\}$ より $\{v_1, v_2, \cdots, v_n\}$ にとり替える変換を与えるから，R^n の自己同型を与える．よって，命題 5.8 より，$Q \in GL_n(R)$ となる．

同様にして，R^m の基底を標準的な基底より $\{u_1, u_2, \cdots, u_m\}$ にとり替える変換を表す行列を (u_{ij}) とする．$(u_{ij}) \in GL_m(R)$ であるから，$P = (u_{ij})^{-1}$ とおくと，P も $GL_m(R)$ の元となる．

f は，基底 $\{v_1, v_2, \cdots, v_n\}$ と $\{u_1, u_2, \cdots, u_m\}$ に関しては，行列



$$E = \left(\begin{array}{ccc|c} e_1 & & 0 & \\ & e_2 & & 0 \\ & & \ddots & \\ 0 & & e_r & \\ \hline & 0 & & 0 \end{array}\right) \quad (0 \neq e_i \in R,\ \ e_i | e_{i+1})$$

の形に表される．他方，A は R^n と R^m の標準的な基底に関して f を表す行列だから，

$$P^{-1} \cdot A = E \cdot Q, \qquad \text{つまり} \qquad A = PEQ$$

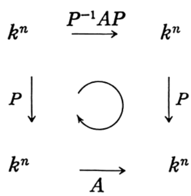
となる．よって，定理の性質をもつ P, Q が存在することがわかった．

一意性は，上の議論を逆にたどると，$\{u_1, u_2, \cdots, u_m\}$ が R^m の基底で，

$$\mathrm{Im}(f) = Re_1u_1 \oplus Re_2u_2 \oplus \cdots \oplus Re_ru_r$$

を満たすことより，定理 5.1 の一意性に帰着する．　　　　　　　　　　　（証明終）

5．3　行列の標準化 II　　k を体とし，$M = k^n$ を長さ n の k に成分をもつ縦ベクトル全体のなす k-ベクトル空間，$A \in M_n(k)$ を $n \times n$ 行列とする．このとき M の基底をとり替え，A の定める線型変換ができるだけ簡単な形で表されるようにすることを考える．このような基底の変換は，行列 $P \in GL_n(k)$ で与えられるから，問題は，$P \in GL_n(k)$ をうまくとることにより，行列



$$P^{-1}AP$$

をできるだけ簡単な形とすることになる．

まず $R = k[x]$ を多項式環とし，$f(x) = \sum_m a_m x^m$ なる R の多項式に対し，

$$f(A) = \sum_m a_m A^m \qquad (A^m \text{ は行列 } A \text{ の } m \text{ 個の積})$$

とおく．このとき $f(A)$ も $M_n(k)$ の行列となるから，

$$R \times M \ni (f(x), x) \longmapsto f(A) \cdot x \in M$$

なる行列の積により，環 R はアーベル群 M に作用する．そこで M を R-加群とみて，その構造を調べる．

M は有限次元 k-ベクトル空間で，$R \supset k$ であるから，M は R-加群としても有限生成である．したがって，$R=k[x]$ は単項イデアル整域だから，定理5.5が使える．M は k-ベクトル空間として有限次元で，$R=k[x]$ は無限次元 k-ベクトル空間であるから，M の直和分解には $R=k[x]$ は現れない．したがって M は，

$$M = M_1 \oplus M_2 \oplus \cdots \oplus M_t\,,$$
$$M_i \simeq k[x]/(f_i(x)) \qquad (f_i(x) \in k[x])$$

の形に書ける．ここで，$k[x]$ の素元は既約多項式だから，$f_i(x)$ は既約多項式のべきの形だとしてよい．

M_i は，M の R-部分加群であるから，

$$A\cdot M_i = x\cdot M_i \subset M_i$$

を満たす．したがって，M の k-ベクトル空間としての基底をこの直和分解に応じてとると，

$$P^{-1}AP = \begin{pmatrix} \boxed{A_1} & & & 0 \\ & \boxed{A_2} & & \\ & & \ddots & \\ 0 & & & \boxed{A_t} \end{pmatrix}$$

の形にブロックに分かれる．ここで A_i は，A の定める M の線型変換を M_i に制限したものの行列としての表現である．

$$f_i(x) = x^h + a_{h-1}x^{h-1} + \cdots + a_1 x + a_0 \qquad (a_j \in k)$$

の形であるとする．このとき，k-ベクトル空間として，

$$M_i \simeq k[x]/(f_i(x)) = k\cdot 1 \oplus k\cdot\bar{x} \oplus \cdots \oplus k\bar{x}^{h-1} \quad (\bar{x}^j = x^j \ (\mathrm{mod}\, f_i(x)))$$

となる．しかも

$$x\cdot\bar{x}^j = \bar{x}^{j+1} \qquad (0 \leqq j < h-1),$$
$$x\cdot\bar{x}^{h-1} = \bar{x}^h = -a_0 - a_1\bar{x} - \cdots - a_{h-1}\bar{x}^{h-1}$$

である．よって，この M_i の基底に関して，

$$A_i = \begin{pmatrix} 0 & 1 & & & & \\ 0 & 0 & 1 & & & \\ \vdots & \vdots & \ddots & \ddots & & \\ 0 & 0 & \cdots & 0 & 1 \\ -a_0 & -a_1 & \cdots & -a_{h-2} & -a_{h-1} \end{pmatrix}$$

と表される．

次に，k が **代数的閉体** であるとする．つまり，$k[x]$ の多項式はすべて1次式の積の形に書けるとする．例えば，複素数体 C は代数的閉体である（代数的閉体については，第Ⅴ章の2.2と5.4参照）．この場合には，既約多項式は1次式に限るから，

$$f_i(x) = (x - \lambda_i)^{n_i} \qquad (\lambda_i \in k)$$

とおける．よって

$$M_i \simeq k[x]/((x - \lambda_i)^{n_i})$$

となる．

$$w = 1 \pmod{f_i(x)} \in k[x]/(f_i(x))$$

とし，$k[x]/(f_i(x))$ の基底として，

$$v_1 = w, \qquad v_2 = (x - \lambda_i)\cdot w, \qquad \cdots, \qquad v_{n_i} = (x - \lambda_i)^{n_i - 1}\cdot w$$

をとる．このとき

$$(x - \lambda_i)\cdot v_j = v_{j+1} \qquad (1 \leqq j \leqq n_i - 1), \qquad (x - \lambda_i) v_{n_i} = 0$$

であるから，

$$A\cdot v_j = \lambda_i v_j + v_{j+1} \qquad (1 \leqq j \leqq n_i - 1), \qquad A\cdot v_{n_i} = \lambda_i \cdot v_{n_j}$$

となる．したがって，M_i のこの基底に関しては，

$$A_i = \begin{pmatrix} \lambda_i & 1 & 0 & & 0 \\ & \lambda_i & 1 & 0 & \\ & & \ddots & \ddots & 0 \\ & & & \ddots & 1 \\ 0 & & & & \lambda_i \end{pmatrix}$$

と表される．これより次の定理を得る．

定理 5.10　kを代数的閉体とし，$A \in M_n(k)$ とする．このとき適当な $P \in GL_n(k)$ をとると，

$$P^{-1}AP = \begin{pmatrix} \boxed{A_1} & & & 0 \\ & \boxed{A_2} & & \\ & & \ddots & \\ 0 & & & \boxed{A_t} \end{pmatrix}, \qquad A_i = \begin{pmatrix} \lambda_i & 1 & & 0 \\ & \lambda_i & 1 & \\ & & \ddots & \ddots \\ & & & 1 \\ 0 & & & \lambda_i \end{pmatrix} \in M_{n_i}(k)$$

の形に表される．しかも，Pのとり方を変えても，ブロック $\{A_1, A_2, \cdots, A_t\}$ の順序が変るのみである．これを**ジョルダンの標準型**とよぶ．

［証 明］　標準型の存在はすでに示した．一意性は，上の議論の逆をたどり，定理 5.5 の一意性に帰着すればよい．　（証明終）

$$A = P\cdot\begin{pmatrix} \lambda & 1 & & 0 \\ & \lambda & 1 & \\ & & \ddots & \ddots \\ 0 & & \ddots & 1 \\ & & & \lambda \end{pmatrix}\cdot P^{-1} \qquad (P \in GL_n(k),\ \lambda \in k)$$

とする．このとき，mに関する帰納法で，

$$A^m = P\cdot\begin{pmatrix} \lambda^m & \binom{m}{1}\lambda^{m-1} & \binom{m}{2}\lambda^{m-2} & \cdots & \binom{m}{n-1}\lambda^{m-n+1} \\ & \lambda^m & \binom{m}{1}\lambda^{m-1} & \cdots & \binom{m}{n-2}\lambda^{m-n+2} \\ & & \lambda^m & & \vdots \\ 0 & & & \ddots & \vdots \\ & & & & \lambda^m \end{pmatrix}\cdot P^{-1}$$

となることが証明できる．一般に，

$$f(x) = a_m x^m + a_{m-1}x^{m-1} + \cdots + a_1 x + a_0 \in k[x]$$

に対して，xにAを代入した

$$f(A) = a_m A^m + a_{m-1}A^{m-1} + \cdots + a_1 A + a_0 E_n \in M_n(k)$$

を計算する．もし k の標数（第V章，例 1.1 参照）が 0 なら，

$$f(A) = P\cdot\begin{pmatrix} f(\lambda) & \frac{1}{1!}f'(\lambda) & \frac{1}{2!}f^{(2)}(\lambda) & \cdots\cdots & \frac{1}{(n-1)!}f^{(n-1)}(\lambda) \\ & f(\lambda) & \frac{1}{1!}f'(\lambda) & \cdots\cdots & \frac{1}{(n-2)!}f^{(n-2)}(\lambda) \\ & 0 & f(\lambda) & & \vdots \\ & & & \ddots & \\ & & & & f(\lambda) \end{pmatrix}\cdot P^{-1}$$

となることがわかる．とくに，$f(A)$ が零行列になるには，

$$f(\lambda) = f'(\lambda) = \cdots = f^{(n-1)}(\lambda) = 0$$

となることが必要十分である．したがって，

$$f(A) = 0 \iff f(x) = (x-\lambda)^n g(x) \qquad (g(x) \in k[x])$$

が成り立つ．また，上の様な A に対して $\det(x\cdot E_n - A)$ を計算すると，

$$\det\begin{pmatrix} x-\lambda & -1 & & & 0 \\ & x-\lambda & -1 & & \\ & & \ddots & \ddots & \\ & 0 & & \ddots & -1 \\ & & & & x-\lambda \end{pmatrix} = (x-\lambda)^n$$

となっている．（この式は，k の標数が 0 でなくても成り立つ．）

$A \in M_n(k)$ が定理 5.10 の様なジョルダンの標準型をもつとする．このとき，多項式 $f(x)$ に対し，

$$f(A) = P\cdot\begin{pmatrix} \boxed{f(A_1)} & & & 0 \\ & \boxed{f(A_2)} & & \\ & & \ddots & \\ 0 & & & \boxed{f(A_t)} \end{pmatrix}\cdot P^{-1}$$

となる．これより，次の命題を得る．

命題 5.11 $A \in M_n(k)$ に対し，A の **固有多項式** を，

$$f_A(x) = \det(x\cdot E_n - A)$$

で定義し，その根を **固有値** とよぶ．このとき，A が定理 5.10 のようなジョ

ルダンの標準型をもつなら，

$$f_A(x) = \prod_{1\leq i\leq t} (x-\lambda_i)^{n_i}$$

となる．したがって，ジョルダンの標準型の対角部には固有値が並ぶ．また，固有多項式 $f_A(x)$ に A を代入すると零行列となる．

問題 5. 12 $R = \boldsymbol{Z}$, $A = \begin{pmatrix} 10 & 4 & 6 \\ 18 & 12 & 30 \end{pmatrix}$ とするとき，A の単因子を求めよ．

(ヒント) R を単項イデアル整域，$A = (a_{ij}) \in M(m, n ; R)$ とする．このとき，

(i) A の第 i 行と第 j 行を入れ替える，

(ii) A の第 i 行の r 倍 $(r \in R)$ を第 j 行に加える，

(iii) A の第 i 行を r 倍 $(r \in U(R))$ する，

および，行の代りに列をとり同じことを行うもの (i′), (ii′), (iii′) を **基本の変形** とよぶ．(i), (ii), (iii) は適当な $U \in GL_m(R)$ を A の左から掛け，(i′), (ii′), (iii′) は適当な $V \in GL_n(V)$ を A の右から掛けることで得られる．

補題 5.4 より，$A = (a_{ij})$ に対し基本の変形を行い，a_{11} が $\{a_{1j}\ (1 \leqq j \leqq n),\ a_{i1}\ (1 \leqq i \leqq m)\}$ の最大公約数になるようにできる．そうすると，(ii), (ii′) を使うことにより，$a_{1j} = 0\ (2 \leqq j \leqq n)$，$a_{i1} = 0\ (2 \leqq i \leqq m)$ とできる．以下 $A' = (a_{ij})_{2\leq i\leq m,\, 2\leq j\leq n}$ に対し同じことを繰り返し行い，A を対角行列とできる．対角部が $a_{11} | a_{ii}$ なる条件を満たすようにするには，すべての行を第 1 行に加え同じことを行えばよい．

なお以上は一般の行列に対しても成り立つようにのべたが，実際の具体的な行列に対しては，その形に応じて，もっと効率的に基本の変形が使える．

問題 5. 13 k を代数的閉体，$A \in M_n(k)$ とするとき，次の 3 つは同値であることを示せ．

(1) A のジョルダンの標準型は対角行列である．

(2) k^n の適当な基底 $\{v_1, v_2, \cdots, v_n\}$ で，$A \cdot v_i = \lambda_i v_i\ (\lambda_i \in k)$ となるものが存在する．

(3) 重根をもたない多項式 $f(x) \in k[x]$ で，$f(A) = 0$ となるものが存在する．

この条件を満たすとき，A は **半単純** であるという．

問題 5. 14 k を代数的閉体で，$A, B \in M_n(k)$ は半単純かつ $A \cdot B = B \cdot A$ を満たすとする．このとき，適当な $P \in GL_n(k)$ をとると，$P^{-1}AP$ と $P^{-1}BP$ が共に対角行列

となることを示せ.

問題 5.15　kを体とするとき，$B \in M_n(k)$ は，適当な正整数mに対し$B^m = 0$となるなら，**べき零**であるという．kが代数的閉体なら，任意の$X \in M_n(k)$ は,

$$X = A + B, \quad A \text{は半単純}, \quad B \text{はべき零}, \quad AB = BA$$

の形に一意的に表されることを示せ.

問題 5.16　Aをn次複素行列とするとき,

$$\exp(A) = \sum_{0 \leq m < \infty} \frac{1}{m!} A^m$$

は$M_n(C)$ の中で収束することを示せ.

§6.　完全可約加群と半単純環*

この§では，完全可約加群の性質と，半単純環の構造を調べる．この§の結果は，§7の定理7.6の証明以後でのみ使う.

6.1　完全可約性　Rを単位元1をもつ環とし，Mを左R-加群とする．このとき，MのR-部分加群がMと$\{0\}$に限るなら，Mは**既約**であるといい，そうでないとき**可約**であるという．この定義は，Mを作用域Rをもつ群と見ての既約性と一致する（第Ⅱ章，§7参照)．以下簡単のため，左(右) R-加群$\{0\}$を0とも表す．次の定理は証明は簡単だが，非常に重要である.

定理6.1（シューアの補題）M, Nを既約な左R-加群とする．このとき，0でない左R-加群の準同型写像$f: M \longrightarrow N$は同型となる．とくに，Mが既約な左R-加群なら，自己準同型環$\mathrm{End}_R(M)$は斜体となる.

[**証明**]　$f: M \longrightarrow N$を定理の通りとする．このとき，$\mathrm{Ker}(f) \subset M$と$\mathrm{Im}(f) \subset N$は，$R$-部分加群をなす．ところが$M, N$が既約で，$f \neq 0$であるから，$\mathrm{Ker}(f) = 0$, $\mathrm{Im}(f) = N$となる．よってfは同型となる．とくに，fは逆写像$f^{-1}: N \longrightarrow M$をもつから，後半も成り立つ.　　　　　　　　　　　　　　　(証明終)

左R-加群Mが，既約なR-部分加群M_i ($i \in I$) の（一般には無限個の）直

和 $M = \bigoplus_{i \in I} M_i$ と表されるなら，M は **完全可約**（または**半単純**）であるという．完全可約性については，次の定理が成り立つ．

定理6.2 M を左 R-加群とする．このとき，

(1) M が完全可約となるための必要十分条件は，M の任意の R-部分加群が，M の直和因子となることである．

(2) M が完全可約なら，M の R-部分加群はすべて完全可約となる．

[**証明**] $M = \bigoplus_{i \in I} M_i$ (M_i は既約) とし，N を M の R-部分加群とする．I の部分集合 J に対し，$M_J = \bigoplus_{i \in J} M_i$，$M_\emptyset = 0$ とおく．$\mathscr{N} = \{J \subset I \mid N \cap M_J = 0\}$ は空集合 $\emptyset$ を含むから $\mathscr{N} \neq \emptyset$ である．$\mathscr{N}$ を包含関係により順序集合とし，その全順序部分集合 $\mathscr{L}$ を任意にとり，$L = \bigcup_{J \in \mathscr{L}} J$ とおく．$x = (x_i) \in M_L \subset \bigoplus_i M_i$ をとると，直和の定義より有限個の i を除き $x_i = 0$ となっている．したがって，M_J の定義より，ある $J \in \mathscr{L}$ に対し $x = (x_i) \in M_J$ となる．よって $M_L = \bigcup_{J \in \mathscr{L}} M_J$ が成り立つ．とくに $N \cap M_L = \bigcup_{J \in \mathscr{L}} (N \cap M_J) = 0$ となり，$L \in \mathscr{N}$ となる．よって $\mathscr{N}$ は帰納的順序集合となる．

ツォルンの補題により，$\mathscr{N}$ には極大元 J が存在する．このとき，$i \notin J$ なら $J \cup \{i\} \notin \mathscr{N}$ となるから，$N \cap (M_J + M_i) \neq 0$ となる．したがって，$(N + M_J) \cap M_i \neq 0$ となる．この式の左辺は M_i の R-部分加群で，M_i は既約だから，$(N + M_J) \cap M_i = M_i$ となる．よって $N + M_J \supset M_i$ となり，$N + M_J \supset M_J + \bigoplus_{i \notin J} M_i = M$ となる．よって $N + M_J = M$，$N \cap M_J = 0$ が成り立つから，$M = N \oplus M_J$ となる．これにより (1) の必要性がわかった．また $N \simeq M/M_J \simeq \bigoplus_{i \notin J} M_i$ だから，(2) が成り立つこともわかった．なお，剰余加群 $M/N \simeq M_J$ の完全可約性にも注意しておく．

次に，M の任意の R-部分加群が M の直和因子をなすと仮定する．N を M の R-部分加群とし，N の R-部分加群 P を任意にとる．そこで $M = P \oplus Q$ と直和に分解し，$Q' = N \cap Q$ とおくと，$N = P \oplus Q'$ が成り立つ．よって N も M と同じ性質をもつ．

$N \neq 0$ とし，$0 \neq x \in N$ をとる．ツォルンの補題により，N の R-部分加群で x を含まないもののうち，極大なもの N_1 を作る．そこで $N = N_1 \oplus N_2$ と直和に分解する．$x \notin N_1$ だから，$N_2 \neq 0$ である．ここで N_2 が既約でないとすると，$N_2 = N_2' \oplus N_2''$ と R-部分加群の直和に分解できる．このとき N_1 のとり方より，$N_1 + N_2' \ni x$，$N_1 + N_2'' \ni x$ だから，$N_1 = (N_1 + N_2') \cap (N_1 + N_2'') \ni x$ となり，$N_1 \not\ni x$ という仮定に矛

盾する．よってN_2は既約となる．とくに，Mの0でないR-部分加群は，既約なR-部分加群を含むことがわかった．

Mの既約なR-部分加群の全体を$\{M_i \mid i \in I\}$とし，Iの部分集合Jで，M_i $(i \in J)$全体が生成するMのR-部分加群が，これらの直和となるもの全体の集合を$\mathscr{N}$とおく．$\mathscr{N}$は帰納的順序集合となり，極大元をもつことが前と同様にしてわかる．$J \in \mathscr{N}$が極大だとし，$M' = \bigoplus_{i \in J} M_i$とおく．もし$M' \neq M$なら，$M = M' \oplus N$なる$R$-部分加群$N \neq 0$と，$N$の既約な$R$-部分加群$M_k$をとる．このとき$J \cup \{k\} \in \mathscr{N}$となるから，これは$J$の極大性に矛盾する．よって$M = M' = \bigoplus_{i \in J} M_i$となる．　　　（証明終）

Mを完全可約な左R-加群とする．もしMがアルティン的またはネター的（第Ⅲ章，§5参照）ならば，Mは有限個の既約な左R-加群の直和$M_1 \oplus M_2 \oplus \cdots \oplus M_l$となる．この場合，$\{M_1, M_2, \cdots, M_l\}$は$M$の組成因子となるから，ジョルダン・ヘルダーの定理（第Ⅱ章，定理8.11）により，同型の差を除き一意的に定まる．

Mを左R-加群とする．このときMの直和因子がMと0に限るなら，Mは**直既約**であるという．Mが直既約であることは，Mの自己準同型環$\mathrm{End}_R(M)$が片側イデアルの直和に分解しないことと同値である．一般に，直既約性については，次の定理が成り立つ（証明は略す）．

定理 6.3　Mを左R-加群とする．このとき，

（1）　Mがアルティン的なら，Mは有限個の直既約なR-部分加群の直和と表される．

（2）　（クルル・シュミットの定理）　Mはアルティン的かつネター的であるとする．また

$$M = M_1 \oplus M_2 \oplus \cdots \oplus M_m = N_1 \oplus N_2 \oplus \cdots \oplus N_n$$

を，Mの2通りの直既約なR-部分加群による直和分解とする．このとき$m = n$で，しかも$\{1, 2, \cdots, m\}$のある置換πで，$M_i \simeq N_{\pi(i)}$，かつ

$$M = N_{\pi(1)} \oplus \cdots \oplus N_{\pi(l)} \oplus M_{l+1} \oplus \cdots \oplus M_m \qquad (l = 1, 2, \cdots, m)$$

となるものが存在する．

6.2　根基　環 R の極大左イデアル全体の交りを R の（ジャコブソン）**根基**とよび，J または $J(R)$ と表す．

M を左 R-加群とするとき，$\mathrm{Ann}(M)=\{a\in R \mid aM=0\}$ は R の両側イデアルとなる．これを M の **零化イデアル** とよぶ．

命題6.4　$J(R)$ は M が既約な左-R 加群全体を動くときの $\bigcap \mathrm{Ann}(M)$ に等しい．したがって $J(R)$ は R の両側イデアルとなる．

[**証明**]　M を既約な左 R-加群，$M\ni m\neq 0$ とする．M は既約だから，$Rm=M$ となり，$R\ni r\longmapsto rm\in M$ は全射で，その核は $\mathrm{Ann}(M)$ と一致する．ところが $M\simeq R/\mathrm{Ann}(M)$ は既約だから，$\mathrm{Ann}(M)$ は極大左イデアルとなる．よって $\mathrm{Ann}(M)\supset J(R)$ となる．

逆に $\mathfrak{m}$ を R の極大左イデアルとすると，$R/\mathfrak{m}$ は既約な左 R-加群で，$\mathfrak{m}\supset \mathrm{Ann}(R/\mathfrak{m})$ となる．よって $\bigcap \mathrm{Ann}(M)\subset \bigcap \mathfrak{m}=J(R)$ となり，$\bigcap \mathrm{Ann}(M)=J(R)$ が成り立つ．
$\mathrm{Ann}(M)$ は R の両側イデアルだから，命題の後半は明らかである．　　（証明終）

補題6.5　有限生成な左 R-加群 $M\neq 0$ は，極大な R-部分加群をもつ．

[**証明**]　$M=Rm_1+Rm_2+\cdots+Rm_r$ とし，M の R-部分加群で M と異なるもの全体のなす集合を $\mathscr{M}$ とし，$\mathscr{M}$ を包含関係により順序集合とする．$\mathscr{M}\ni 0$ だから $\mathscr{M}\neq\emptyset$ である．$\mathscr{L}$ を $\mathscr{M}$ の全順序部分集合とし，$L=\bigcup_{N\in\mathscr{L}} N$ とおく．もし $L=M$ なら，$L=\bigcup_{N\in\mathscr{L}} N\ni m_i$ $(1\leqq i\leqq r)$ となる．そこで $m_i\in N_i\in\mathscr{L}$ とし，（$\mathscr{L}$ が全順序集合であるから）N_k が $N_1, N_2, \cdots, N_r$ の中で最大であるとする．このとき $N_k\ni m_1, m_2, \cdots, m_r$ となり，$N_k=M$ となる．これは矛盾だから，$L\subsetneqq M$ となり，$\mathscr{M}$ は帰納的となる．よって，ツォルンの補題により，$\mathscr{M}$ は極大元をもつ．　　（証明終）

次の命題は東屋と中山によるものだが，応用上非常に重要である．

命題6.6　（中山の補題）　M を有限生成な左 R-加群，N を M の R-部分加群とする．このとき，$M=N+J(R)M$ が成り立てば，$N=M$ となる．したがって，$M=J(R)M$ なら $M=0$ となる．

[**証明**]　M の代りに M/N を考えることにより，命題の前半は後半より従う．よって $M=J(R)M$ だとする．

$M \neq 0$ とし，補題6.5より M の極大部分群 M_1 をとる．M/M_1 は既約だから，命題6.4より $J(R)(M/M_1) = 0$ となる．よって $M = J(R)M \subset M_1$ となり矛盾である．

(証明終)

命題6.7 (1) R の元 r が $J(R)$ に属することと，任意の R の元 s に対し，$1-sr$ が左逆元をもつこととは同値である．

(2) $J(R)$ は，次の条件を満たす R の両側イデアル $\mathfrak{a}$ の中で，最大のものである：

$$(\text{☆}) \qquad r \in \mathfrak{a} \implies 1-r \text{ は可逆元である．}$$

(3) $J(R)$ は，R の極大右イデアル全体の共通部分に等しい．

[証明] (1) $r \in J(R)$, $s \in R$ とし，$R(1-sr) = R$ を示す．そこで $R(1-sr) \subsetneq R$ とすると，III章，問題2.4により $R(1-sr)$ を含む極大左イデアル $\mathfrak{m}$ が存在する．このとき $sr \in J(R) \subset \mathfrak{m}$, $1-sr \in \mathfrak{m}$ となり，$1 = (1-sr) + sr \in \mathfrak{m}$ となり矛盾する．逆に $r \notin J(R)$ とすると，r を含まない R の極大左イデアル $\mathfrak{m}$ が存在する．このとき $Rr + \mathfrak{m} = R$ となり，$ar + b = 1$ ($a \in R$, $b \in \mathfrak{m}$) と書ける．よって $1 - ar = b \in \mathfrak{m}$ であるから，$R(1-ar) \subset \mathfrak{m} \subsetneq R$ となり，$1-ar$ は左逆元をもたない．

(2) $r \in J(R)$ とし，(1) より $a(1-r) = 1$ となる $a \in R$ をとる．このとき $a = 1-(-a)r$ だから，(1) より $ba = 1$ となる $b \in R$ が存在する．このとき $b = b\{a(1-r)\} = (ba)(1-r) = 1-r$ であるから，$(1-r)a = 1$ となる．よって $1-r$ は可逆元となり，$J(R)$ は (☆) を満たす．

$\mathfrak{a}$ が (2) の条件を満たすものとし，$r \in \mathfrak{a}$ を任意にとる．$s \in R$ とすると $sr \in \mathfrak{a}$ だから，$1-sr$ は可逆元である．よって (1) より $r \in J(R)$ となり，$\mathfrak{a} \subset J(R)$ となる．

(3) (2) の性質 (☆) は左右対称だから，$J(R)$ は極大右イデアル全体の交りとも一致する．

(証明終)

環 R の元 r は，適当な自然数 n をとると $r^n = 0$ となるとき**べき零**であるという．R の左(右，両側)イデアル $\mathfrak{a}$ は適当なべきをとると $\mathfrak{a}^n = 0$ となるとき，**べき零左(右，両側)イデアル**であるという．

系6.8 $\mathfrak{a}$ をべき零元から成る R の左(または右)イデアルとすると，$\mathfrak{a} \subset J(R)$ となる．

[証 明] 仮定より，$r \in \mathfrak{a}$, $s \in R$ とすると $sr \in \mathfrak{a}$ となり，ある n に対し $(sr)^n = 0$ となる．よって $(1 - sr)\cdot\{1 + (sr) + (sr)^2 + \cdots + (sr)^{n-1}\} = 1$ となり，命題6.7 の (1) より $r \in J(R)$ となる． (証明終)

定 理 6. 9 R を左アルティン環とすると，その根基 $J(R)$ は R の最大のべき零左イデアルとなる．

[証 明] $\mathfrak{a}$ をべき零左イデアルとすると，任意の $a \in \mathfrak{a}$ も元としてべき零となり，$J(R)$ に属する．よって系6.8より，$J(R)$ がべき零であることを示せばよい．

R は左アルティン環だから，$J(R) \supset J(R)^2 \supset \cdots$ なる列に降鎖律を使い，ある n より $J(R)^n = J(R)^{n+1} = \cdots$ となることがわかる．$J(R)^n \neq 0$ とし，R の左イデアル $\mathfrak{a}$ で $J(R)^n\mathfrak{a} \neq 0$ となるものの全体を $\mathscr{A}$ とする．$J(R) \in \mathscr{A}$ だから $\mathscr{A} \neq \emptyset$ である．R は左アルティン環だから，$\mathscr{A}$ は極小元 $\mathfrak{a}_0$ をもつ．$J(R)^n\{J(R)\mathfrak{a}_0\} = J(R)^{n+1}\mathfrak{a}_0 = J(R)^n\mathfrak{a}_0 \neq 0$ だから，$J(R)\mathfrak{a}_0 \in \mathscr{A}$ となる．ところが $J(R)\mathfrak{a}_0 \subset \mathfrak{a}_0$ だから，極小性より $J(R)\mathfrak{a}_0 = \mathfrak{a}_0$ となる．また極小性より，$a \in \mathfrak{a}_0$ が $J(R)^n a \neq 0$ を満たすとすると，$\mathfrak{a}_0 = Ra$ となる．よって中山の補題より $\mathfrak{a}_0 = 0$ となる．これは矛盾だから，$J(R)^n = 0$ となる．

(証明終)

系 6. 10 可換アルティン環の（ジャコブソン）根基は，べき零根基（第Ⅲ章，6.1参照）と一致する．

6. 3 半単純環 以下次の2つの定理を証明する．

定 理 6. 11 環 R について次の (1)〜(5) は同値である．

(1) すべての左 R-加群は完全可約である．

(2) すべての左 R-加群は射影的である．

(3) R は左アルティン的で，$J(R) = 0$ である．

(4) R は左アルティン的で，有限個の単純環の直和となる．

(5) 斜体 $D_1, D_2, \cdots, D_r$ を適当にとると，$R \simeq M_{n_1}(D_1) \oplus M_{n_2}(D_2) \oplus \cdots \oplus M_{n_r}(D_r)$ となる．

定理 6.12 環 R について次の (a)〜(c) は同値である.

(a) R は左アルティン的単純環である.

(b) R は斜体 D 上の行列環 $M_n(D)$ と同型になる.

(c) R の極小左イデアルは互いに同型であり, R は極小左イデアル有限個の直和として表される.

R が定理 6.11 の性質を満たすとき, R を **半単純環** であるという. R を環とし $J(R)$ を R の根基とすると, $R/J(R)$ の根基は準同型定理により 0 となる. よって定理 6.11 より,

系 6.13 R を左アルティン環とすると, $R/J(R)$ は半単純環となる.

[定理 6.11 と定理 6.12 の証明] 定理 6.2 の (1) と例 3.5 より, 定理 6.11 の (1) と (2) は共に, 任意の左 R–加群の任意の R–部分加群が直和因子となることを意味するから, 互いに同値である.

斜体 D 上の行列環 $M_n(D)$ は, III 章, 例 1.2 により単純環となる. また $M_n(D)$ は D 上 n^2 次元のベクトル空間をなし, その左イデアルは D–部分空間となるから, (次元を考えることにより) $M_n(D)$ が降鎖律を満たすことがわかる. よって $M_n(D)$ は左アルティン環であり, このようなものの有限個の直和である $M_{n_1}(D_1)\oplus M_{n_2}(D_2)\oplus\cdots\oplus M_{n_r}(D_r)$ も左アルティン環である. よって (5) $\Longrightarrow$ (4) と (b) $\Longrightarrow$ (a) がわかった.

一般に, 根基の定義より, $J(R_1\oplus R_2\oplus\cdots\oplus R_r)\subset J(R_1)\oplus J(R_2)\oplus\cdots\oplus J(R_r)$ が成り立つ (実は等号となる). また R が単純環なら, $J(R)=0$ となる. よって (4) $\Longrightarrow$ (3) が成り立つ.

R を左アルティン環で, $J(R)=0$ だとする. $\mathscr{M}$ を R の極大左イデアルの全体とすると, $\bigcap_{\mathfrak{m}\in\mathscr{M}}\mathfrak{m}=J(R)=0$ となる. ところが R は左アルティン的だから, $\mathscr{M}$ の有限個の元の交り $\mathfrak{m}_1\cap\mathfrak{m}_2\cap\cdots\cap\mathfrak{m}_n$ ($\mathfrak{m}_i\in\mathscr{M}$) の全体を $\mathscr{N}$ とすると, $\mathscr{N}$ は極小元をもつ. それを $\mathfrak{m}_1\cap\mathfrak{m}_2\cap\cdots\cap\mathfrak{m}_n$ とすると, $\bigcap_{\mathfrak{m}\in\mathscr{M}}\mathfrak{m}=0$ だから, 極小性より $\mathfrak{m}_1\cap\mathfrak{m}_2\cap\cdots\cap\mathfrak{m}_n=0$ となる. したがって $R\longrightarrow R/\mathfrak{m}_1\oplus R/\mathfrak{m}_2\oplus\cdots\oplus R/\mathfrak{m}_n$ なる自然な写像は, 左 R–加群の単射な準同型となる. ここで各 $R/\mathfrak{m}_i$ は既約であるから, 定理 6.2, (2) より, R 自身は左 R–加群とみて完全可約である. ところが例 1.4 より, 任意の左 R–加群は R–

自由加群を R-部分加群で割ったものと同型となる．よって，定理 6.2 より，任意の左 R-加群は完全可約となる．よって (3) $\Longrightarrow$ (1) がわかった．

一般に，R を環とするとき，

$$j: \quad \mathrm{End}_R(R) \ni f \longmapsto f(1) \in R$$

なる写像は，

$$(f+g)(1) = f(1) + g(1), \qquad (f \circ g)(1) = f(g(1)) = g(1)f(1)$$

を満たす．ところが $\forall x \in R$ に対し，$f(y) = y \cdot x$ ($\forall y \in R$) とおくと，$f \in \mathrm{End}_R(R)$ で $f(1) = x$ となるから，j は全射である．また $f(y) = f(y \cdot 1) = y \cdot f(1)$ ($\forall y \in R$) であるから，j は単射である．よって j は，環の(積の順序を逆にする)逆同型である．そこで R の代りに $\mathrm{End}_R(R)$ の構造を調べる．

R が条件 (1) を満たすとする．このとき R 自身 R-加群とみて完全可約となり，既約な R-部分加群の直和となる．ここで R の R-部分加群とは，環 R の左イデアルのことであるから，R は左 R-加群とみて極小左イデアルの直和 $\bigoplus_{i \in I} \mathfrak{a}_i$ の形となる．そこで単位元 $1 \in R$ のこの直和に対応した分解を $1 = \sum_{i \in I} 1_i$ とすると，有限個の i 以外は $1_i = 0$ となる．よって，$R = 1R = \bigoplus_{I \in i} 1_i \mathfrak{a}_i$ であるから，R は有限個の極小左イデアルの直和となる．そこでこれらの極小左イデアルのうち，左 R-加群として同型なものをまとめ，$\mathfrak{a}_i$ の n 個の直和を $n\mathfrak{a}_i$ と表し，

$$R \simeq n_1\mathfrak{a}_1 \oplus n_2\mathfrak{a}_2 \oplus \cdots \oplus n_r\mathfrak{a}_r, \qquad \mathfrak{a}_i \not\simeq \mathfrak{a}_j \quad (i \neq j)$$

と表す．R が (c) を満たす場合も，$r = 1$ としてこのことは成り立つ．

$\mathfrak{a}_i$ は既約だから，$n_i\mathfrak{a}_i \supset (n_i - 1)\mathfrak{a}_i \supset \cdots \supset \mathfrak{a}_i \supset 0$ は左 R-加群 $n_i\mathfrak{a}_i$ の組成列を与え，これ以上真の細分をもたない．よってシュライアーの細分定理（II章，定理 8.8）により，$n_i\mathfrak{a}_i$ の任意の R-部分加群は $\mathfrak{a}_i$ のいくつかの直和と同型となる．$n_i\mathfrak{a}_i$ の剰余加群についても同様である．

そこで $i \neq j$ とすると $\mathfrak{a}_i \not\simeq \mathfrak{a}_j$ であるから，準同型の核および像の組成因子を考えると，$\mathrm{Hom}_R(n_i\mathfrak{a}_i, n_j\mathfrak{a}_j) = 0$ となることがわかる．よって

$$\mathrm{End}_R(R) \simeq \mathrm{End}_R(n_1\mathfrak{a}_1) \oplus \mathrm{End}_R(n_2\mathfrak{a}_2) \oplus \cdots \oplus \mathrm{End}_R(n_r\mathfrak{a}_r)$$

となる．明らかに

$$\mathrm{End}_R(n_i\mathfrak{a}_i) \simeq M_{n_i}(\mathrm{End}_R(\mathfrak{a}_i))$$

である．ところが，各 $\mathfrak{a}_i$ は既約だから，定理 6.1 より $D_i = \mathrm{End}_R(\mathfrak{a}_i)$ は斜体となる．よって (1) $\Longrightarrow$ (5) が成り立つことがわかった．また (c) $\Longrightarrow$ (b) が成り立つこ

ともわかった．さらに，（単純環）R の極小イデアルで互いに同型なものが2つ以上あると，上の議論より $\mathrm{End}_R(R)$ は斜体上の行列環の2つ以上の直和と同型となることがわかる．これは R が単純環であるということに矛盾するから，単純環のすべての極小左イデアルは同型となる．これで定理6.11と定理6.12の証明が完成した．　　（証明終）

（注）　定理6.11，定理6.12ではすべて左 R-加群としての性質の形でのべたが，定理6.11,（5）と定理6.12,（b）は左右対称だから，定理の左 R-加群としての性質を，対応する右 R-加群としての性質におき直しても成り立つ．

次に，定理6.11の応用として次の定理を示す．

定理6.14　左アルティン環は左ネター環である．

［証明］　R を左アルティン環とし，$J=J(R)$ を R の根基とする．定理6.9より $J(R)$ はべき零だから，$R\supset J\supset J^2\supset\cdots\supset J^n=0$ なる列が得られる．ここで $\bar{R}=R/J$ は，系6.13より，半単純な左アルティン環となる．また $J^{(i)}=J^i/J^{i+1}$ $(0\leqq i\leqq n-1)$ は $J\cdot J^{(i)}=0$ を満たすから，左 $\bar{R}$-加群とみなせる．定理6.11,（1）より $J^{(i)}$ は完全可約な左 $\bar{R}$-加群で，左アルティン環 R の左イデアル J^i の剰余加群だから，極小条件を満たす．よって $J^{(i)}$ は有限個の既約な $\bar{R}$-加群の直和となる．したがって，$J^{(i)}$ は $\bar{R}$-加群とみて組成列をもつが，これは R-加群とみても組成列である．よって $R\supset J\supset J^2\supset\cdots\supset J^n=0$ において，各 $J^{(i)}=J^i/J^{i+1}$ は組成列をもつから，環 R は左 R-加群として組成列をもつ．よって第Ⅱ章，定理8.12より，環 R は左 R-加群とみてネター的となり，R は左ネター環となる．　　（証明終）

問題6.15　D_1, D_2 を斜体とするとき，

$$M_{n_1}(D_1)\simeq M_{n_2}(D_2)\iff n_1=n_2,\ D_1\simeq D_2$$

が成り立つことを示せ．

問題6.16　R を半単純環とし，M を既約な左 R-加群とする．このとき $R/\mathrm{Ann}(M)$ は，R を $R_1\oplus R_2\oplus\cdots\oplus R_s$ と単純環の直和に分解したときの，どれかの R_i に環として同型であり，さらに M は，R_i の極小左イデアル（定理6.12,（c）参照）と左 R-加群として同型となることを示せ．

§7. 多元環とその表現

この§では，多元環とその表現についての基礎的概念を定義し，さらに，§6の結果を使って，有限群の表現の性質を調べる.

7.1 多元環　Rを可換環とする．このとき，R-加群Aの上に積・が定義され，この積が分配法則と，

$$(r\cdot a)\cdot b = a\cdot(r\cdot b) = r\cdot(a\cdot b) \qquad (r\in R,\ a,b\in A)$$

を満たすとき，AをR上の**分配多元環**とよぶ．分配的多元環が積・に関し結合法則を満たし，さらに単位元をもつなら，AをR上の（**結合的**）**多元環**とよぶ（第I章，例7.4参照)．多元環は環をなす.

（注）Rが体Kで，AがK上の分配多元環なら，AはK-ベクトル空間をなす．そこでAのK上の次元が有限次元だとすると，例1.3より，AはK-加群としてネター的かつアルティン的となる．とくに，Aが体K上の有限次元の多元環なら，Aは左アルティン環となり，§6の結果が使える.

例 7.1　R上の分配多元環Aにおいて，その演算が

$$a\cdot a=0, \qquad (a\cdot b)\cdot c+(b\cdot c)\cdot a+(c\cdot a)\cdot b=0 \quad (\textbf{ヤコビの等式})$$

を満たすなら，Aは**リー代数**であるという．例えばDを斜体，$A=M_n(D)$とし，行列の積・を使って

$$[X, Y]=X\cdot Y-Y\cdot X \qquad (X, Y\in A)$$

とおくと，これによりAはリー代数となる．リー代数は，リー群や代数群を研究する場合に非常に重要である.

例 7.2　R上の分配的多元環Aにおいて，

$$a\cdot b=b\cdot a, \qquad a^2\cdot(b\cdot a)=(a^2\cdot b)\cdot a$$

が成り立つとき，Aを**ジョルダン代数**とよぶ．例えば，Aが結合的多元環のとき，$\{a,b\}=a\cdot b+b\cdot a$　とおくと，これによりAはジョルダン代数となる.

結合的でない多元環の中にも，リー代数のような重要なものが存在するが，以下の話は結合的多元環に限る.

A を R 上の多元環とする．このとき A の部分集合 B が A の演算により多元環をなすなら，B を A の **部分多元環** であるという．これは，

$$B+B\subset B,\qquad B\cdot B\subset B,\qquad R\cdot B\subset B,\qquad 1\in B$$

を意味する．例えば，$R\cdot 1_A=\{r\cdot 1_A\mid r\in R\}$ は A の部分多元環をなす．

A を多元環とし，$\mathfrak{a}$ を A の両側イデアルとする．このとき剰余環 $A/\mathfrak{a}$ の上には，

$$r\cdot(a+\mathfrak{a})=r\cdot a+\mathfrak{a}\qquad (r\in R,\ a\in A)$$

により R-加群の構造が入り，R 上の多元環となる．これを **剰余多元環** とよぶ．

A, B を共に R 上の多元環とする．このとき $f: A\longrightarrow B$ が多元環の **準同型** であるとは，f が環の準同型であり，かつ R-加群の準同型にもなることをいう．$f: A\longrightarrow B$ が多元環の準同型なら，$\mathrm{Im}(f)$ は B の部分多元環をなし，かつ多元環としての同型 $A/\mathrm{Ker}(f)\simeq\mathrm{Im}(f)$ が成り立つ．

A を基底 $\{u_i\}$ をもつ R-自由加群とする．したがって，A の任意の元は $\sum_i r_iu_i$ $(r_i\in R)$ の形に一意的に表されるものとする．もし A が R 上の分配多元環となれば，A における積は，基底の間の積を線型に拡張したものとなる．よって，

$$u_iu_j=\sum_k\gamma_{ijk}u_k\qquad (\gamma_{ijk}\in R)$$

とおき $\{\gamma_{ijk}\}$ を定めると，積 $A\times A\longrightarrow A$ が一意的に定まる．この $\{\gamma_{ijk}\}$ を A の基底 $\{u_i\}$ に関する **構造定数** とよぶ．もし A の積が結合法則を満たすなら，$(u_iu_j)u_k=u_i(u_ju_k)$ より

$$\sum_p\gamma_{ijp}\gamma_{pkl}=\sum_q\gamma_{jkq}\gamma_{iql}\qquad (\forall i,j,k,l)$$

が成り立つ．逆に構造定数がこの等式を満たすなら，A の積は結合法則を満たす．

例 7. 3 $\alpha,\beta\in R,\ \neq 0$ とし，A を基底 $\{e_0,e_1,e_2,e_3\}$ をもつ R-自由加群とする．このとき，e_0 を単位元 1 とし，$\alpha,\beta\in R\setminus\{0\}$ をとり，

$$e_1{}^2=\alpha,\qquad e_2{}^2=\beta,\qquad e_3{}^2=-\alpha\beta$$

$$e_1e_2=-e_2e_1=e_3,\qquad e_2e_3=-e_3e_2=-\beta e_1,\qquad e_3e_1=-e_1e_3=-\alpha e_2$$

とおくと，A には多元環の構造が入る．これを **四元数環** とよぶ．

四元数環の元は　$q=\xi_0e_0+\xi_1e_1+\xi_2e_2+\xi_3e_3$ $(\xi_i\in R)$　の形に一意的に表され，共役　$\bar{q}=\xi_0e_0-\xi_1e_1-\xi_2e_2-\xi_3e_3$，トレース　$q+\bar{q}=2\xi_0$，ノルム　$q\bar{q}=\xi_0{}^2-\alpha\xi_1{}^2-\beta\xi_2{}^2+\alpha\beta\xi_3{}^2$　等が定義される．

R が実数体 $\boldsymbol{R}$ であり，$\alpha=\beta=-1$ のときは，$q\bar{q}=\xi_0{}^2+\xi_1{}^2+\xi_2{}^2+\xi_3{}^2\geqq 0$　となるから，この多元環は斜体となる．これを **ハミルトンの四元数環** とよぶ．

例 7. 4　G を群とし，G の元を基底とする R-自由加群を A とする．A の任意の元は，$\sum_{\sigma\in G}a_\sigma\cdot\sigma$ $(a_\sigma\in R)$ の形に一意的に表される．ここで A の基底 $\{\sigma\mid\sigma\in G\}$ には G での演算により，結合法則を満たす積が定まっている．したがって，この G での積を線型に拡張することにより，A に結合法則を満たす積が定まり，これにより A は R 上の多元環となる．これを $R[G]$ で表し，群 G の R 上の **群環** とよぶ（例 4. 8 参照）．

7. 2　多元環の表現　　R を可換環とし，A を R 上の多元環とする．R-加群 M の上に A の作用が定義され，これにより M が左 A-加群となり，かつ

$$r(am)=(ra)m=a(rm)\qquad(r\in R,\ a\in A,\ m\in M)$$

が成り立つとき，M を **多元環 A 上の加群** という．

M を R-加群とするとき，R 上の多元環としての準同型

$$\rho:\quad A\longrightarrow \mathrm{End}_R(M)$$

を M を **表現加群** とする多元環 A の **表現** という．M が多元環 A 上の加群なら，

$$\rho(a)m=am\qquad(a\in A,\ m\in M)$$

とおくと，ρ は $A\longrightarrow\mathrm{End}_R(M)$ なる多元環の準同型を定め，Mを表現加群とする A の表現ができる．逆に $\rho:A\longrightarrow\mathrm{End}_R(M)$ を多元環 A の表現とすると，A の M への作用が

$$am=\rho(a)m\qquad(a\in A,\ m\in M)$$

により定まり，M は多元環 A 上の加群となる．

$\rho: A \longrightarrow \mathrm{End}_R(M)$ と $\rho': A \longrightarrow \mathrm{End}_R(M')$ を多元環 A の表現とする．このとき，M と M' が A 上の加群として同型なら，ρ と ρ' は **同値** であるといい，$\rho \sim \rho'$ と表す．このことは，R–加群としての同型 $i: M \longrightarrow M'$ で，

$$i(\rho(a)m) = \rho'(a)i(m) \qquad (a \in A,\ m \in M)$$

を満たすものが存在することを意味する．これは，

$$\rho(a) = i^{-1} \circ \rho'(a) \circ i \qquad (a \in A)$$

とも書ける．

$\rho: A \longrightarrow \mathrm{End}_R(M)$ を多元環 A の表現とし，N を M の A–部分加群とする．このとき N と M/N も多元環 A 上の加群となり，これらを表現加群とする A の表現が得られる．これらを ρ の **部分表現** および **商表現** とよぶ．

例 7. 5　A を R 上の多元環とする．このとき A 自身は，A の左からの乗法により，多元環 A の表現加群となる：

$$\rho(a)m = am \qquad (a \in A,\ m \in A).$$

これを A の **左正則表現** という．**右正則表現** も同様にして定義される．

G を群とし，$R[G]$ を G の可換環 R 上の群環とする．M を R–加群とするとき，群の準同型

$$\rho: \quad G \longrightarrow \mathrm{Aut}_R(M)$$

を，群 G の M を表現加群とする **表現** という．

ρ を群 G の M 上の表現とすると，これを線型に拡張することにより，群環 $R[G]$ の表現

$$\rho: \quad R[G] \longrightarrow \mathrm{End}_R(M), \qquad \rho(\sum_\sigma a_\sigma \sigma) = \sum_\sigma a_\sigma \rho(\sigma)$$

が得られる．逆に $\rho: R[G] \longrightarrow \mathrm{End}_R(M)$ が多元環 $R[G]$ の表現なら，これを制限して群 G の表現 $\rho: G \longrightarrow \mathrm{Aut}_R(M)$ が得られる．

定 理 7. 6　（マシュケ）　G を位数 g の有限群，K を標数が（0か）g と素な体（第Ⅴ章，例 1.1 参照）とする．このとき，G の K–加群による表現はすべて完全可約であり，群環 $K[G]$ は半単純環となる．

[証明] 多元環 $K[G]$ 上の加群は，左 $K[G]$-加群である．したがって，定理 6.11 より，任意の左 $K[G]$-加群が射影的なことを示せば十分である．

M, Nを左 $K[G]$-加群とし，$f: M \longrightarrow N$ を全射な準同型とする．Kは体だから，$K \ni k \longmapsto k\cdot 1 \in K[G]$ は単射であり（III章，命題 1.1 参照)，$K \simeq K\cdot 1_{K[G]}$ である．そこで M, Nを K-加群とみなすと，Kは体だから，例 1.3 よりこれらは自由加群となる．よって命題 3.3 より K-加群の準同型 $h: N \longrightarrow M$ で $f\circ h = \mathrm{id}_N$ となるものが存在する．そこで $i: N \longrightarrow M$ を，

$$i(n) = g^{-1}\sum_{\sigma\in G}\sigma h(\sigma^{-1}n) \qquad (n \in N)$$

とおき定義する．これは K の標数が g と素だから定義され，

$$i(\tau n) = g^{-1}\sum_{\sigma}\sigma h(\sigma^{-1}\tau n) = g^{-1}\sum_{\tau^{-1}\sigma}\tau(\tau^{-1}\sigma)h((\tau^{-1}\sigma)^{-1}n) = \tau i(n)$$

$$(f\circ i)(n) = g^{-1}\sum_{\sigma}\sigma(f\circ h)(\sigma^{-1}n) = g^{-1}\sum_{\sigma}\sigma(\sigma^{-1}n) = n$$

が成り立つ．よって，iは左 $K[G]$-加群の準同型で，$f\circ i = \mathrm{id}_N$ を満たすから，N は射影的となる． (証明終)

例 7. 7 Kを体とし，Aを K 上有限次元の半単純な多元環，Mを有限次元の Kベクトル空間とし，A の Mでの表現 ρを考える．$A = A_1 \oplus A_2 \oplus \cdots \oplus A_s$ を A の単純環の直和としての表現とし，$1_A = e_1 + e_2 + \cdots + e_s$ を対応する A の単位元の中心直交べき等元の和としての表示とする（III章，1.3 参照)．そこで $M_i = \rho(e_i)M$ とおくと，M_iは M の A-部分加群で，M_i の上に Aは $\rho_i: A_i \longrightarrow \mathrm{Aut}_K(M_i)$ の形で作用する．A_iは単純環だから，問題 6.16 より M_iは，A_i の極小左イデアルを $\mathfrak{a}_i$ とすると，$n_i\mathfrak{a}_i$ ($\exists n_i \geqq 0$) と左 A_i-加群として同型である．

一般に，Aを体 K 上の多元環，$\rho: A \longrightarrow \mathrm{Aut}_K(M)$ を A の有限次元 K-ベクトル空間 Mでの表現とする．M_i の基底 $\{u_i\}_{1\leq i\leq n}$をとり，これにより ρから $\tilde{\rho}: A \longrightarrow GL_n(K)$ なる行列表現を作り，

$$\mathrm{tr}\,\rho(a) = \mathrm{tr}\,\tilde{\rho}(a) \qquad (a \in A)$$

($\mathrm{tr}\,\tilde{\rho}(a)$ は行列 $\tilde{\rho}(a) = (a_{ij})$ のトレース $\sum_{1\leq i\leq n} a_{ii}$) とおく．行列のトレースは，

$$\mathrm{tr}(PAP^{-1}) = \mathrm{tr}(A) \qquad (A \in M_n(K),\ P \in GL_n(K))$$

を満たすから，これは M_i の K-ベクトル空間の基底 $\{u_i\}$ のとり方によらない．$\mathrm{tr}\,\rho: A \longrightarrow K$を表現 ρ の **指標** とよぶ．

Kを標数 0 の体（V章，例 1.1 参照）とし，Aを K 上の有限次元の半単純な多元環とする．そこで，$A = A_1 \oplus A_2 \oplus \cdots \oplus A_s$，$1 = e_1 \oplus e_2 \oplus \cdots \oplus e_s$，$M = M_1 \oplus M_2 \oplus \cdots$

$\oplus M_s$, $\rho = \rho_1 \oplus \rho_2 \oplus \cdots \oplus \rho_s$ などを前の通りとする．このとき $\mathrm{tr}\,\rho = \mathrm{tr}\,\rho_1 + \mathrm{tr}\,\rho_2 + \cdots + \mathrm{tr}\,\rho_s$ で，とくに，

$$\mathrm{tr}\,\rho(e_i) = \mathrm{tr}\,\rho_i(e_i) = (\dim_K M_i)\cdot 1_K$$

が成り立つ．ところが K の標数は 0 だから，$\mathrm{tr}\,\rho$ を定めると $\dim_K M_i$ が定まり，$M_i \simeq n_i\mathfrak{a}_i$ となる n_i が定まる．よって M_i の左 R_i–加群としての同型類が定まる．したがって，K を標数 0 の体，A を K 上の有限次元の半単純な多元環とすると，A の有限次元 K–ベクトル空間での表現 $\rho: A \longrightarrow \mathrm{Aut}_K(M)$ は，その指標 $\mathrm{tr}\,\rho: A \longrightarrow K$ により同値類が定まる．

7．3　有限群の表現*　　G を有限群とし，$A = \boldsymbol{C}[G]$ を G の複素数体 $\boldsymbol{C}$ 上の群環とする．このとき，G の有限次元 $\boldsymbol{C}$–ベクトル空間での表現と，群環 A の有限次元 $\boldsymbol{C}$–ベクトル空間での表現は同一視できる（7.2 参照）．また $\boldsymbol{C}$ は標数 0 の体だから，定理 7.6 より，A は半単純環となる．よって定理 6.11 により，すべての左 A–加群は完全可約となる．したがって，有限群 G の有限次元の $\boldsymbol{C}$–ベクトル空間での表現は完全可約となり，既約表現の直和となる．また例 7.7 より，任意の既約な左 A–加群は，A のある単純成分の極小左イデアルと左 A–加群として同型である．したがって，

定理 7．8　有限群 G の有限次元 $\boldsymbol{C}$–ベクトル空間での表現は既約表現の直和と同値である．また G の任意の複素既約表現は，群環 $\boldsymbol{C}[G]$ での左正則表現の中に既約成分として含まれる．

次に，$\rho: G \longrightarrow \mathrm{Aut}_{\boldsymbol{C}}(M)$ を，有限群 G の有限次元 $\boldsymbol{C}$–ベクトル空間での表現とする．このとき，ρ を群環の表現とみて作った $\mathrm{tr}\,\rho: \boldsymbol{C}[G] \longrightarrow \boldsymbol{C}$ を G に制限したものを，$\mathrm{tr}\,\rho: G \longrightarrow \boldsymbol{C}$ で表し，G の表現 ρ の **指標** とよぶ．$\boldsymbol{C}$ の標数は 0 だから，例 7.7 より，

定理 7．9　$\rho: G \longrightarrow \mathrm{Aut}_{\boldsymbol{C}}(M)$ を，有限群 G の有限次元 $\boldsymbol{C}$–ベクトル空間での表現とする．このとき ρ の同値類は，その指標 $\mathrm{tr}\,\rho$ により一意的に定まる．

$\mathrm{tr}\,\rho : G \longrightarrow \boldsymbol{C}$ を上の通りとする．このとき，

$$(\mathrm{tr}\,\rho)(aga^{-1}) = \mathrm{tr}\,\rho(aga^{-1}) = \mathrm{tr}\{\rho(a)\rho(g)\rho(a)^{-1}\} = \mathrm{tr}\,\rho(g) \qquad (a, g \in G)$$

である．よって指標 $(\mathrm{tr}\,\rho)(g)$ は，$g \in G$ の共役類にしかよらない．

有限群 G の有限次元ベクトル空間での表現 ρ の指標 $\mathrm{tr}\,\rho$ を以下単に G の **指標** とよび，とくに ρ が既約のとき **既約指標** とよぶ．このとき，次のことが証明できる（第Ⅱ章末，問題9参照）：

（1） χ, δ を有限群 G の既約指標とする．このとき，

$$\sum_{g \in G} \chi(g)\delta(g^{-1}) = \begin{cases} \sharp(G) & (\chi, \delta \text{ が同値のとき}) \\ 0 & (\text{その他}) \end{cases}$$

が成り立つ（**指標の第1直交関係**）．

（2） $X(G)$ で有限群 G の既約指標の全体を表すとき，

$$\sum_{\chi \in X(G)} \chi(g)\chi(h^{-1}) = \begin{cases} \sharp\, C_G(g) & (g, h \text{ が共役のとき}) \\ 0 & (\text{その他}) \end{cases}$$

となる（**指標の第2直交関係**）．ここで $C_G(g)$ は $g \in G$ の G の中での中心化群 $\{k \in G \mid kg = gk\}$ を表す．

有限群 G の上の関数 $\varphi : G \longrightarrow \boldsymbol{C}$ で，$\varphi(g)$ $(g \in G)$ が G の中での g の共役類にしかよらないものを，G 上の **類関数** とよぶ．G の指標は類関数であり，G 上の類関数の全体は，高々［G の共役類の個数］を次元とする $\boldsymbol{C}$-ベクトル空間をなす．ところが，指標の第2直交関係より，$h \in G$ に対し，

$$\varphi_h(g) = \sharp\, C_G(h)^{-1} \sum_{\chi \in X(G)} \chi(g)\chi(h^{-1})$$

とおくと，$\varphi_h(g)$ は g と h が共役のとき1となり，その他のときは0となる．よって，既約指標の全体 $X(G)$ は，類関数の全体を $\boldsymbol{C}$-ベクトル空間として生成する．

そこで，φ, ψ を G 上の類関数とするとき，その **内積** を

$$(\varphi, \psi) = \sharp\,(G)^{-1} \sum_{g \in G} \varphi(g)\psi(g^{-1})$$

で定める．このとき，指標の第1直交関係より，既約指標の全体 $X(G)$ は正規直交基底をなすことがわかる．

問　題

1. 左 R–加群 M の R–部分加群 N_1, N_2 について，N_1+N_2 と $N_1\cap N_2$ が有限生成なら，N_1, N_2 も有限生成であることを示せ．

2. D を環とする．このとき，D が斜体をなすことと，すべての左 D–加群が D–自由加群となることは同値であることを示せ．

（ヒント）十分性は，D の極大左イデアル $\mathfrak{l}$ をとり，$D/\mathfrak{l}$ を考える．

3. $M=\boldsymbol{Z}/m\boldsymbol{Z},\ N=\boldsymbol{Z}/n\boldsymbol{Z}$ $(m, n\in \boldsymbol{N})$ とするとき，$M\otimes_{\boldsymbol{Z}} N$ と $\mathrm{Hom}_{\boldsymbol{Z}}(M, N)$ を求めよ．

4. $R=\boldsymbol{Z}$ とし，R–加群 $M_1=\boldsymbol{Q},\ M_2=\boldsymbol{Q}/\boldsymbol{Z},\ M_3=\boldsymbol{Z}/p\boldsymbol{Z}$（$p$ は素数）を考える．これらのうち，ねじれ加群，可除加群，射影加群，入射加群，平坦加群となるものをあげよ．

5. R を環，Q を左 R–加群とする．R の任意の左イデアル $\mathfrak{l}$ より R への自然なうめ込み $\iota:\mathfrak{l}\to R$ の定める準同型 $\iota^*:\mathrm{Hom}_R(R, Q)\longrightarrow \mathrm{Hom}_R(\mathfrak{l}, Q)$ が全射なら，Q は入射的であることを示せ．

（注）命題 3.4,（2）より，Q が入射的ならこの条件は満たされる．

6. R を可換環，M, N を R–加群，$\mathscr{M}=\{\mathfrak{m}\}$ を R の極大イデアル全体のなす集合とする．次の（1),（2）を示せ．

（1）$i_{\mathfrak{m}}: M\longrightarrow M_{\mathfrak{m}}=R_{\mathfrak{m}}\otimes_R M$ を極大イデアル $\mathfrak{m}$ による局所化とする．このとき，

$$\prod_{\mathfrak{m}\in\mathscr{M}} i_{\mathfrak{m}}:\quad M\longrightarrow \prod_{\mathfrak{m}\in\mathscr{M}} M_{\mathfrak{m}}$$

は単射となる．

（2）$f: M\longrightarrow N$ なる R–加群の準同型が単射（全射）になるための必要かつ十分な条件は，すべての $\mathfrak{m}\in\mathscr{M}$ につき，$f_{\mathfrak{m}}: M_{\mathfrak{m}}\longrightarrow N_{\mathfrak{m}}$ が単射（全射）となることである．

7.　(1)　Rを環，M, M'を有限生成な射影的左R-加群，$\mathfrak{a}$をRの根基に含まれる両側イデアルとする．このとき，$M/\mathfrak{a}M$と$M'/\mathfrak{a}M'$が左$R/\mathfrak{a}$-加群として同型なら，MとM'は左R-加群として同型であることを示せ．

(2)　局所環上の有限生成射影的加群は，自由加群となることを示せ．

8.　Mを左R-加群，$n \in \boldsymbol{Z}$, $n \geqq 0$ とする．このとき，次の3条件は同値なことを示せ．

(1)　任意の左R-加群Nについて，$\mathrm{Ext}_R^{n+1}(M, N) = 0$ となる．

(2)　$$0 \longrightarrow P_n \longrightarrow P_{n-1} \longrightarrow \cdots \longrightarrow P_0 \longrightarrow M \longrightarrow 0$$

なる左R-加群の完全列において，$P_0, P_1, \cdots, P_{n-1}$が射影的なら$P_n$も射影的である．

(3)　$$0 \longrightarrow P_n \longrightarrow P_{n-1} \longrightarrow \cdots \longrightarrow P_0 \longrightarrow M \longrightarrow 0$$

なる形のMの射影的分解が存在する．

(ヒント)　(1) $\Longrightarrow$ (2) については，(2)の完全列において，$A_i = \mathrm{Ker}(\partial_{i-1}) = \mathrm{Im}(\partial_i)$, $A_0 = M$, $A_n = P_n$ とおく．そこで短完全列

$$0 \longrightarrow A_{j+1} \longrightarrow P_j \longrightarrow A_j \longrightarrow 0$$

から，Ext の完全列を作り，jに関する帰納法で，$\mathrm{Ext}_R^1(A_j, N) = 0$ を示す．Ext の完全列より，任意のNに対し $\mathrm{Ext}_R^1(M, N) = 0$ となるなら，Mは射影的である．

9.　単項イデアル整域R上の加群Mについて，次のことを示せ．

(1)　Mが平坦となるための必要十分条件は，Mが0以外のねじれ元を持たないことである．

(2)　Mが入射的となるための必要十分条件は，Mが可除加群となることである．

10.　例7.3で定義した四元数環

$$A = Re_0 + Re_1 + Re_2 + Re_3$$

において，Rが標数が2でない体K（第V章，例1.1参照）だとする．このとき，

(1)　Aの元　$q = \xi_0 e_0 + \xi_1 e_1 + \xi_2 e_2 + \xi_3 e_3$ ($\xi_i \in K$)　をとるとき，$e_1^{-1} q e_1$, $e_2^{-1} q e_2$, $e_3^{-1} q e_3$ を求めよ．

(2)　Aは中心がKの単純環であることを示せ．

(3)　$N(q) = q\bar{q} = \xi_0^2 - \alpha\xi_1^2 - \beta\xi_2^2 + \alpha\beta\xi_3^2$ が0になるのが$q = 0$のときに限るなら，Aは斜体であり，0以外の元$q \in A$に対し$N(q) = 0$となるなら，Aは行列環$M_2(K)$と同型となることを示せ．

V　体

集合 K が，加法 $+$ と乗法・に関し，単位元 1 と零元 0 $(1 \neq 0)$ をもつ環になるものとする．このとき，演算・が可換で，かつ K の 0 以外の任意の元 a が，乗法・に関する逆元 a^{-1} をもつとき，K を体とよぶ（第Ⅰ章，§6 参照）．この章では体の性質を調べ，またガロアの理論についても学ぶ．

なおこの章では，第Ⅰ章，第Ⅱ章，第Ⅲ章の結果は使うが，第Ⅳ章の結果は，ベクトル空間の話以外はほとんど使わない．

§1.　体の拡大

1.1　体の拡大　　有限個の元から成る体を **有限体** とよび，無限個の元から成る体を **無限体** とよぶ．

L を体とするとき，L の部分集合 K が L の和と積に関して体をなすとき，K を L の **部分体**，L を K の **拡大体** であるという．このとき L と K の組を，**拡大** L/K などとも表す．また，$L \supset M \supset K$ なる L の部分体 M を，L/K の **中間体** とよぶ．

例 1.1　L を体とし，1_L をその単位元とする．このとき，

$$f:\quad \boldsymbol{Z} \ni n \longmapsto n1_L \in L$$

は環の準同型である．よって，環として $\boldsymbol{Z}/\mathrm{Ker}(f) \simeq \mathrm{Im}(f)$ となるが，L は体だからその部分環 $\mathrm{Im}(f)$ は整域となる．よって，$\mathrm{Ker}(f) = 0$ または $p\boldsymbol{Z}$（p は素数）となる（第Ⅲ章，例 2.3 参照）．そこでこれに応じて，L の **標数** は 0 または p であるという．

L の標数が 0 であるとすると，f は単射であり，L は $\boldsymbol{Z}$ と同型な部分環を含む．よって，($R = \boldsymbol{Z}$，$S = \boldsymbol{Z} \setminus \{0\}$ として第Ⅲ章，定理 3.2 を使うと，) L は有理数体 $\boldsymbol{Q}$ と同型

な部分体 K を含むことがわかる.

L の標数が $p>0$ なら, $\mathrm{Im}(f)\simeq \boldsymbol{Z}/p\boldsymbol{Z}$ は体となる. これを K で表す.

いずれの場合も, K は L の部分体で, 任意の L の部分体に含まれる. この K を L の **素体** とよぶ.

L/K を体の拡大とする. このとき,

$$K\times L\ni (k,l)\ \longmapsto\ k\cdot l\in L \qquad (\text{右辺は } L \text{ での積})$$

なる作用により, L は体 K 上のベクトル空間とみなせる. そこで, K–ベクトル空間 L の次元 (第Ⅳ章, 例 1.3 参照) を $[L:K]$ で表す. したがって, $[L:K]=n<+\infty$ であるとは, 適当な L の元 $\omega_1,\omega_2,\cdots,\omega_n$ があり, L の任意の元が,

$$a_1\omega_1+a_2\omega_2+\cdots+a_n\omega_n \qquad (a_i\in K)$$

の形に一意的に表されることを意味する. $[L:K]<+\infty$ のとき, 拡大 L/K は **有限次拡大** であるという.

命 題 1.2　M を拡大 L/K の中間体であるとすると, 次式が成り立つ:

$$[L:K]=[L:M][M:K]$$

[証 明]　$[L:M]=m<\infty$, $[M:K]=n<\infty$ であるとし, M–ベクトル空間 L の基底を $\{\alpha_1,\alpha_2,\cdots,\alpha_m\}$, K–ベクトル空間 M の基底を $\{\beta_1,\beta_2,\cdots,\beta_n\}$ とする. このとき L の任意の元は,

$$\sum a_{ij}\,\alpha_i\,\beta_j \qquad (1\leqq i\leqq m,\ 1\leqq j\leqq n,\ a_{ij}\in K)$$

の形に一意的に表される. よって $\{\alpha_i\beta_j\}$ は K–ベクトル空間 L の基底となり, $[L:K]=mn$ が成り立つ.

$[L:M]$ または $[M:K]$ が無限のときは, $[L:K]$ も無限となる.　(証明終)

L を体とする. このとき L の 0 以外の元は単数となるから, L のイデアルは, L と $\{0\}$ に限る (第Ⅲ章, 命題 1.1 参照). よって, L_1, L_2 を体, $f:L_1\longrightarrow L_2$ を環の準同型とすると, L_1 のイデアルである $\mathrm{Ker}(f)$ は $\{0\}$ に一致する. つまり, 体から体への環準同型は単射となる. この場合, f は体 L_1 から L_2 の**中への同型**であるという. とくに, f が全射のときは, f は L_1 から L_2

の **上への同型** であるといい，$f: L_1 \simeq L_2$ などと表す．

L_1, L_2 を体 K の拡大体であるとする．このとき，$f: L_1 \longrightarrow L_2$ なる中への（上への）同型で，$f|_K = \mathrm{id}$ となるものを，L_1 から L_2 の **中への（上への）K-同型**であるという．

体 L から L の上への同型全体を $\mathrm{Aut}(L)$, 拡大 L/K から L/K の上への K-同型の全体を $\mathrm{Aut}(L/K)$ と表す．これらは写像の合成により，群となる．

K を L の部分体，S を L の部分集合とする．このとき，K と S を含む L の最小の部分体を $K(S)$ で表し，K 上 S で **生成** される体，または K に S を **添加** してできる体という．L/K の中間体 M は，適当な有限集合 S をとると $M = K(S)$ となるとき，K 上 **有限生成** であるという．とくに，M が K 上1つの元 θ で生成されるとき，$M = K(\theta)$ は **単拡大** であるという．

S_1, S_2 を L の部分集合とする．このとき $K(S_1)(S_2)$ は L/K の中間体で，S_1, S_2 を含み，$K(S_1 \cup S_2)$ に含まれるから，$K(S_1 \cup S_2) = K(S_1)(S_2)$ が成り立つ．

S を L の部分集合とする．このとき，F が S の有限部分集合を動くとき，和 $\bigcup_F K(F)$ は S を含む K の部分体で，$K(S)$ に含まれるから，$K(S) = \bigcup_F K(F)$ が成り立つ．したがって一般の $K(S)$ を知るには，$K(F)$ がわかればよいが，これについて次の命題が成り立つ．

命題 1.3 L/K を体の拡大とし，$\theta_1, \theta_2, \cdots, \theta_n \in L$ とする．このとき，K 上 $\theta_1, \theta_2, \cdots, \theta_n$ が生成する体 $K(\theta_1, \theta_2, \cdots, \theta_n)$ は，

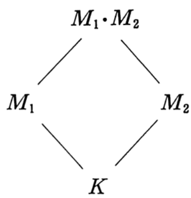
$$f(\theta_1, \theta_2, \cdots, \theta_n)/g(\theta_1, \theta_2, \cdots, \theta_n)$$
$$(f, g \in K[x_1, x_2, \cdots, x_n],\ g(\theta_1, \theta_2, \cdots, \theta_n) \neq 0)$$

の形の L の元全体から成る．

［証 明］ $\theta_1, \theta_2, \cdots, \theta_n \in K(\theta_1, \theta_2, \cdots, \theta_n)$ であるから，それらより作られる $f(\theta_1, \theta_2, \cdots, \theta_n)/g(\theta_1, \theta_2, \cdots, \theta_n)$ も $K(\theta_1, \theta_2, \cdots, \theta_n)$ に入る．ところが，この形の $K(\theta_1, \theta_2, \cdots, \theta_n)$ の元全体は加減乗除で閉じており，体をなす．よって $K(\theta_1, \theta_2, \cdots, \theta_n)$ と一致する．

（証明終）

拡大 L/K の中間体 M_1, M_2 が与えられたとする．このとき，$M_1 \cup M_2$ で生成される L/K の中間体 $K(M_1 \cup M_2)$ を $M_1 \cdot M_2$ で表し，M_1 と M_2 の **合成体** とよぶ．またこの場合，$M_1 \cdot M_2 = M_1(M_2)$ であるから，拡大 $M_1 \cdot M_2/M_1$ を拡大 M_2/K の M_1 への **持ち上げ** ともいう．



1.2 単拡大の性質　一般の拡大は，単拡大を繰り返し作ることにより得られる．この意味で，体の拡大の性質を調べるとき，単拡大の研究が基礎となる．

L/K を体の拡大とし，θ を L の元，$M = K(\theta)$ とおく．$R = K[x]$ を K 上の一変数多項式環とし，x に θ を代入する環の準同型写像

$$\varphi: \quad R = K[x] \ni f(x) \longmapsto f(\theta) \in M$$

を考える．R は単項イデアル環だから，そのイデアルである $\mathrm{Ker}(\varphi)$ は単項イデアルとなる（第Ⅲ章，例 4.6 参照）．よって $\mathrm{Ker}(\varphi) = \{0\}$ となるか，$\mathrm{Ker}(\varphi)$ は最高次の係数が 1 の多項式

$$\mathrm{Irr}(\theta, K, x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \qquad (a_i \in K)$$

で生成される．

$\mathrm{Ker}(\varphi) = \{0\}$ とする．$\varphi: R \longrightarrow M$ は単射であるから，第Ⅲ章，定理 3.2 により，$R = K[x]$ の商体 $K(x)$ からの準同型写像

$$\tilde{\varphi}: \quad K(x) \ni f(x) \longmapsto f(\theta) \in M$$

に拡張される．$\tilde{\varphi}$ は体から体への環準同型だから単射である．また命題 1.3 より，$M = K(\theta)$ の任意の元は $f(\theta)$ の形に書けるから，$\tilde{\varphi}$ は全射である．よって $\mathrm{Ker}(\varphi) = \{0\}$ なら，$\tilde{\varphi}: K(x) \longrightarrow M$ は上への K-同型となる．

$\mathrm{Ker}(\varphi) \neq \{0\}$ とする．このとき，上のような $\mathrm{Irr}(\theta, K, x)$ は θ と K にのみより一意的に定まる．これを θ の **最小多項式** とよび，$n = \deg \mathrm{Irr}(\theta, K, x)$ を θ の **次数** とよぶ．

この場合，φ は

$$\bar{\varphi}: \quad K[x]/(\mathrm{Irr}(\theta, K, x)) \longrightarrow K(\theta)$$

なる単射をひきおこす．ところが $K(\theta)$ は体であるから，イデアル $(\mathrm{Irr}(\theta, K, x))$ は素イデアルとなり，$\mathrm{Irr}(\theta, K, x)$ は既約多項式となる．したがって，第Ⅲ章，補題 4.5 より，$(\mathrm{Irr}(\theta, K, x))$ は $K[x]$ の極大イデアルとなり，$K[x]/(\mathrm{Irr}(\theta, K, x))$ は体となる．したがって，$\mathrm{Im}\,\bar{\varphi} \simeq K[x]/(\mathrm{Irr}(\theta, K, x))$ は θ を含む体であるから，$K(\theta)$ と一致し，$\bar{\varphi}$ は上への K-同型となる．とくに φ は全射となる．

以上をまとめると，次の定理を得る．

定理 1.4 K を体，$K(\theta)$ を K の単拡大とする．このとき $K(\theta)$ は，有理関数体 $K(x)$ と同型であるか，多項式環 $K[x]$ の既約多項式 $\mathrm{Irr}(\theta, K, x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$ による剰余環 $K[x]/(\mathrm{Irr}(\theta, K, x))$ と同型となる．

以下，$K(\theta) \simeq K(x)$ のとき θ を K 上 **超越的** であるといい，そうでないとき θ を K 上 **代数的** であるという．

一般に，K の拡大体の元 $\theta_1, \theta_2, \cdots, \theta_n$ は，適当な 0 でない多項式 $f(x_1, x_2, \cdots, x_n) \in K[x_1, x_2, \cdots, x_n]$ で $f(\theta_1, \theta_2, \cdots, \theta_n) = 0$ を満たすものが存在するとき，K 上 **代数的に従属** であるといい，そうでないとき，K 上 **代数的に独立** であるという．

命題 1.5 K を体，θ を K 上代数的な元とし，その次数が n であるとする．このとき $[K(\theta) : K] = n$ で，$K(\theta)$ の任意の元は，

$$c_0 + c_1\theta + \cdots + c_{n-1}\theta^{n-1} \qquad (c_i \in K)$$

の形に一意的に表される．

［証明］ θ の最小多項式を $f(x)$ とする．このとき $\deg f(x) = n$ で，任意の多項式 $g(x) \in K[x]$ は

$$g(x) = q(x)f(x) + r(x) \qquad (q(x), r(x) \in K[x],\ \deg r(x) < n)$$

の形に一意的に表される．よって

$$\psi:\quad K[x]\ni g(x)\longmapsto r(x)\in K[x]$$

なる K–ベクトル空間の準同型写像は，

$$\bar{\psi}:\quad K[x]/(f(x))\xrightarrow{\sim} K+Kx+\cdots+Kx^{n-1}$$

なる K–ベクトル空間の同型をひきおこす．したがって，定理 1.4 の証明より，

$$\bar{\varphi}\circ(\bar{\psi})^{-1}:\quad K+Kx+\cdots+Kx^{n-1}\longrightarrow K(\theta)$$

は K–ベクトル空間の同型である．$\bar{\varphi}$ は x に θ を代入することにより得られたから，このことは，命題が成り立つことを示している．　　(証明終)

θ を K 上代数的な元とすると，$f(x)=\mathrm{Irr}(\theta,K,x)$ は K 上の既約多項式となった．そこで逆に，

$$f(x)=a_nx^n+a_{n-1}x^{n-1}+\cdots+a_1x+a_0\qquad(a_i\in K)$$

が $K[x]$ において既約であるとする．このとき K の拡大体 M で，適当な M の元 θ をとると

$$M=K(\theta),\qquad f(x)=c\cdot\mathrm{Irr}(\theta,K,x)\qquad(c\in K)$$

となるものを，$f(x)$ の **根体** とよぶ．

命題 1.6　任意の $K[x]$ の既約多項式 $f(x)$ に対して，その根体は存在し，K–同型の差を除き一意的に定まる．

［**証明**］ $f(x)$が既約だとすると，剰余環 $K[x]/(f(x))$ は体となる（第Ⅲ章，補題 4.5 参照）．これが根体となることは，定義より明らかである．次に M を $f(x)$ の根体とし，θ を上の通りとする．このとき，環の準同型

$$\varphi:\quad K[x]\ni g(x)\longmapsto g(\theta)\in M$$

は，$M=K(\theta)$ だから全射であり，$f(x)=c\cdot\mathrm{Irr}(\theta,K,x)$ であるから，K–同型 $\bar{\varphi}$：$K[x]/(f(x))\xrightarrow{\sim} M$ をひきおこす．よって，根体は K–同型の差を除き一意的に定まる．

(証明終)

例 1.7　L/K を体の拡大，M を中間体，$\theta\in L$ とする．θ が K 上代数的なら，その K 上の最小多項式を $f(x)$ とすると，θ は $f(x)\in M[x]$ の根となる．よって命題 1.5

より，

$$[M(\theta):M] \leqq \deg f(x) = [K(\theta):K]$$

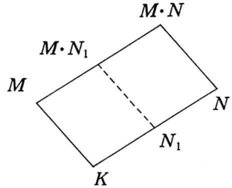
となる．θ が K 上超越的なら $[K(\theta):K]=\infty$ だから，その場合も $[M(\theta):M] \leqq [K(\theta):K]$ が成り立つ．

M, N を L/K の中間体とする．(N が K 上有限生成でないと $[N:K]=\infty$ となることに注意すると，）命題 1.2 と，N の生成元の個数に関する帰納法により，

$$[M\cdot N:M] \leqq [N:K]$$

が成り立つことがわかる．したがって

$$[M\cdot N:K] = [M:K][M\cdot N:M]$$
$$\leqq [M:K][N:K]$$



も成り立つ．ここで等号が成り立つのは，

(LD)　N の元 $a_1, a_2, \cdots, a_n$ が K 上一次独立なら，$a_1, a_2, \cdots, a_n$ は M 上でも一次独立である．

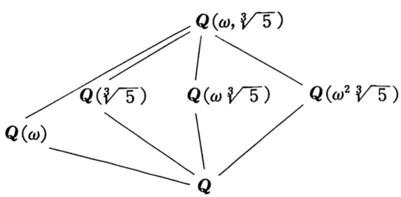
が成り立つときである．この場合，M と N は K 上 **線型無関連** であるという．M と N が線型無関連なら，N と M も線型無関連であることが証明できる．

例 1．8　(1)　$K=\boldsymbol{Q}$, $L=\boldsymbol{C}$, $\theta=3+2\sqrt{-1}$ とおく．このとき $\mathrm{Irr}(\theta,K,x)=x^2-6x+13$, $K(\theta)=\boldsymbol{Q}+\boldsymbol{Q}(3+2\sqrt{-1})=\boldsymbol{Q}+\boldsymbol{Q}\sqrt{-1}$　となる．

(2)　$K=\boldsymbol{Q}$, $L=\boldsymbol{C}$, $f(x)=x^3-5$　とおく．このとき $\omega=(-1+\sqrt{-3})/2$ とおくと，$\sqrt[3]{5}$，$\omega\sqrt[3]{5}$，$\omega^2\sqrt[3]{5}$ が $f(x)$ の L における根となり，$M_1=\boldsymbol{Q}(\sqrt[3]{5})$，$M_2=\boldsymbol{Q}(\omega\sqrt[3]{5})$，$M_3=\boldsymbol{Q}(\omega^2\sqrt[3]{5})$　の 3 つが $f(x)$ の根体となる．このうち M_1 は $\boldsymbol{R}$ に入るが，他の 2 つは $\boldsymbol{R}$ に入らない．また $i \neq j$ のとき，

$$M_i\cdot M_j = \boldsymbol{Q}(\omega, \sqrt[3]{5})$$

となるから，



$$[M_i : K] = 3 \gneqq 2 = [M_i \cdot M_j : M_j]$$

が成り立つ．したがって，M_i と M_j は K 上線型無関連ではない．

§2. 代数拡大と代数的閉体

2.1 代数拡大 L/K を体の拡大とする．このとき，L の任意の元が K 上代数的となるなら，拡大 L/K は **代数拡大** である，または **代数的** であるという．代数拡大であるかどうかの判定には，次の定理およびその系が便利である．

定理 2.1 L/K を体の拡大とする．このとき L/K が有限次拡大であるための必要十分条件は，L/K が有限生成の代数拡大となることである．

[証明] （必要性） L/K を有限次拡大とし，$L \neq K$ であるとする．そこで $\theta_1 \in L$, $\theta_1 \notin K$ を任意にとり，以下 $\theta_{i+1} \in L$, $\theta_{i+1} \notin K(\theta_1, \theta_2, \cdots, \theta_i)$ を帰納的にとってゆく．このとき，帰納法により，

$$\begin{aligned}[K(\theta_1, \theta_2, \cdots, \theta_i, \theta_{i+1}) : K] &= [K(\theta_1, \theta_2, \cdots, \theta_i)(\theta_{i+1}) : K(\theta_1, \theta_2, \cdots, \theta_i)] \\ &\quad \times [K(\theta_1, \theta_2, \cdots, \theta_i) : K] \\ &\geqq 2 \cdot [K(\theta_1, \theta_2, \cdots, \theta_i) : K] \geqq 2^{i+1}\end{aligned}$$

が成り立つ．ところが

$$[K(\theta_1, \theta_2, \cdots, \theta_i, \theta_{i+1}) : K] \leqq [L : K] < +\infty$$

であるから，この操作は有限回で終り，ある n に対し $L = K(\theta_1, \theta_2, \cdots, \theta_n)$ が成り立つ．

$L \ni \theta$ を任意にとる．このとき

$$[K(\theta) : K] \leqq [L : K] < +\infty$$

である．ところが，θ が K 上超越的なら，$K(\theta) \simeq K(x)$ の元 $1, \theta, \theta^2, \cdots$ は K 上 1 次独立だから $K(\theta)$ の K 上の次数は無限大となる．よって，θ は K 上代数的である．

（十分性） $L = K(\theta_1, \theta_2, \cdots, \theta_n)$ で，各 θ_i は K 上代数的であるものとし，その最小多項式を $f_i(x) \in K[x]$ とする．$K_0 = K$, $K_i = K(\theta_1, \theta_2, \cdots, \theta_i)$ とおくと，θ_i は $f_i(x) \in K_{i-1}[x]$ の根だから，

$$[L : K] = [K_n : K_{n-1}][K_{n-1} : K_{n-2}] \cdots [K_1 : K_0]$$

$$= [K_{n-1}(\theta_n) : K_{n-1}][K_{n-2}(\theta_{n-1}) : K_{n-2}]\cdots[K_0(\theta_1) : K_0]$$
$$\leqq \deg f_n \deg f_{n-1} \cdots \deg f_1 < \infty$$

となる．よって L/K は有限次拡大である．　　　　　　　　　　　　（証明終）

系 2.2　L を K の拡大体，$S \subset L$ とし，S の任意の元は K 上代数的であるとする．このとき，$K(S)$ は K 上代数的で，$K(S)$ の元は S の元の K 係数の多項式として表される．

[証明]　F を S の任意の有限部分集合を動かすとき，$K(S) = \bigcup_F K(F)$ が成り立つ．ところが，定理より，$K(F)$ は K 上代数的となる．よって $K(S) = \bigcup_F K(F)$ も K 上代数的となる．後半については，$F = \{\theta_1, \theta_2, \cdots, \theta_n\}$ とすると，命題1.5より，

$$K(F) = K(\theta_1, \theta_2, \cdots, \theta_{n-1})(\theta_n) = K(\theta_1, \theta_2, \cdots, \theta_{n-1})[\theta_n]$$
$$= \cdots = K(\theta_1)[\theta_2]\cdots[\theta_n] = K[\theta_1][\theta_2]\cdots[\theta_n] = K[\theta_1, \theta_2, \cdots, \theta_n]$$

が成り立つ．　　　　　　　　　　　　（証明終）

系 2.3　拡大 L/K の元 α, β が K 上代数的なら，$\alpha \pm \beta$，$\alpha\beta$，α/β $(\beta \neq 0)$ も K 上代数的となる．

[証明]　系2.2より，$K(\alpha, \beta)$ は K 上代数的であり，しかも $\alpha \pm \beta$，$\alpha\beta$，$\alpha/\beta \in K(\alpha, \beta)$ である．　　　　　　　　　　　　（証明終）

命題 2.4　L/K を体の拡大，M をその中間体とする．このとき，L/K が代数拡大となるための必要十分条件は，L/M，M/K が共に代数拡大となることである．

[証明]　L/K が代数的なら，M $(\subset L)$ の任意の元は K 上代数的で，L の任意の元は M $(\supset K)$ 上でも代数的となる．そこで，L/M および M/L が代数的であるとする．θ を L の任意の元とし，θ の M 上の最小多項式を，

$$\mathrm{Irr}(\theta, M, x) = x^n + \alpha_{n-1}x^{n-1} + \cdots + \alpha_1 x + \alpha_0 \qquad (\alpha_i \in M)$$

とする．このとき，例1.7と定理2.1より，

$$[K(\theta) : K] \leqq [K(\alpha_0, \alpha_1, \cdots, \alpha_{n-1}, \theta) : K]$$
$$= [K(\alpha_0, \alpha_1, \cdots, \alpha_{n-1})(\theta) : K(\alpha_0, \alpha_1, \cdots, \alpha_{n-1})][K(\alpha_0, \alpha_1, \cdots, \alpha_{n-1}) : K]$$
$$= [M(\theta) : M][K(\alpha_1, \alpha_2, \cdots, \alpha_{n-1}) : K] < +\infty$$

となる．よってθはK上代数的となる．　(証明終)

系 2.5　L/Kの中間体M_1, M_2がK上代数的なら，合成体$M_1 \cdot M_2$もK上代数的となる．

［証 明］　仮定より，$M_1 \cdot M_2$はM_2上代数的，M_2はK上代数的となる．(証明終)

2.2　代数的閉体　　L/Kを体の拡大とし，$\bar{K}_L$でK上代数的なLの元全体のなす集合を表す．これは，系2.3より体となり，また命題2.4より，Lの元で$\bar{K}_L$上代数的な元は$\bar{K}_L$の元に限る．この$\bar{K}_L$を，以下L**における**K**の代数的閉包**という．また拡大L/Kにおいて，$\bar{K}_L = K$となるとき，KはLにおいて**代数的に閉じている**という．とくに，Kの代数拡大がKに限るなら，Kは任意の拡大体において代数的に閉じている．この場合，Kは**代数的閉体**であるという．

命 題 2.6　体Kが代数的閉体となるための必要十分条件は，次のどれかが成り立つことである．

（a）　$K[x]$の既約多項式は1次式に限る．

（b）　$K[x]$の定数でない多項式は，1次式の積として表される．

（c）　$K[x]$の定数でない多項式は，Kにおいて根をもつ．

［証 明］　第I章，§9で調べたことより，(a)〜(c)は同値である．そこで，これらが必要十分条件であることを示す．

Kを代数的閉体とし，$f(x) \in K[x]$が既約であるとする．このとき，$f(x)$の根体$K[x]/(f(x))$はKの$\deg f(x)$次の代数拡大となるから，仮定より$\deg f(x) = 1$となる．逆に(a)が成り立つなら，任意のK上代数的な元θについて，その最小多項式$\mathrm{Irr}(\theta, K, x)$は1次式となる．よって$\theta \in K$となり，$K$は代数的閉体となる．

(証明終)

系 2.7　体の拡大L/Kにおいて，Lが代数的閉体なら，$\bar{K}_L$も代数的閉体となる．

[証 明] $f(x) \in \bar{K}_L[x]$, $\notin \bar{K}_L$ をとると，これは L において根 θ をもつ．ところが θ は $\bar{K}_L$ 上代数的だから，K 上でも代数的である．よって θ は $\bar{K}_L$ に属する．したがって $f(x)$ は，$\bar{K}_L$ において根をもつ． (証明終)

一般に，体 K が与えられたとき，K の代数拡大で代数的閉体となるものを，単に K の **代数的閉包** とよぶ．$\bar{K}$ が K の代数的閉包で，$L \supset \bar{K}$ なら，$\bar{K}_L = \bar{K}$ となる．

代数的閉体については，次の定理が基本的である．

定理 2.8 （シュタイニッツ） （1） Kを任意の体とするとき，K の代数的閉包が存在する．

（2） $\bar{K}_1, \bar{K}_2$ をそれぞれ体 K_1, K_2 の代数的閉包とする．このとき $\sigma : K_1 \cong K_2$ なる体の同型は，$\bar{\sigma} : \bar{K}_1 \cong \bar{K}_2$ なる同型に拡張できる．とくに，体 K の任意の 2 つの代数的閉包は，K–同型となる．

[証 明] （1） Mを任意の体とするとき，$M[x]^*$ で定数でない M 係数多項式全体のなす集合を表す．このとき，M の代数拡大 E_M で，$M[x]^*$ の任意の元が E_M で少なくとも 1 根をもつようなものを作る．

各 $f(x) \in M[x]^*$ に対し，文字 X_f を作り，その全体を S とする．S の有限個の元に関する M 係数の多項式全体を $M[S]$ で表す．$M[S]$ には自然に和と積が定義され環となるが，そこで $\{f(X_f) \mid f \in M[x]^*\}$ 全体で生成される $M[S]$ のイデアル $\mathfrak{a}$ を考える．

もし $\mathfrak{a} = M[S]$ となるなら，$f_1(x), f_2(x), \cdots, f_n(x) \in M[x]^*$ と $g_1, g_2, \cdots, g_n \in M[S]$ で

$$(*) \qquad g_1 f_1(X_{f_1}) + g_2 f_2(X_{f_2}) + \cdots + g_n f_n(X_{f_n}) = 1$$

となるものが存在する．ここで，$g_1, g_2, \cdots, g_n$ に現れる S の元は有限個だから，$g_1, g_2, \cdots, g_n \in M[X_{f_1}, X_{f_2}, \cdots, X_{f_n}, \cdots, X_{f_N}]$ と仮定する．

$L_0 = K$ とおく．そこで帰納的に，$f_i(x) \in L_{i-1}[x]$ を既約因子に分解し，その 1 つの既約因子の L_{i-1} 上の根体を L_i とおく．このとき，$L = L_n$ は各 $f_i(x)$ の根 θ_i を含む．そこで

$$X_{f_1} = \theta_1, \quad X_{f_2} = \theta_2, \quad \cdots, \quad X_{f_n} = \theta_n, \quad X_{f_{n+1}} = \cdots = X_{f_N} = 0$$

とおき（*）式に代入すると，$0=1$ となり矛盾を生じる．

よって $\mathfrak{a} \subsetneqq M[S]$ であるから，$\mathfrak{a}$ を含む $M[S]$ の極大イデアル $\mathfrak{m}$ が存在する．そこで $E_M = M[S]/\mathfrak{m}$ とおくと，E_M は体で，$\theta_f = X_f \pmod{\mathfrak{m}} \in E_M$（$f \in M[x]^*$）とおくと，$\theta_f \in E_M$ は $f(\theta_f) = 0$ を満たす．

K を定理の通りとし，$K_0 = K$，$K_1 = E_K$ とおく．以下帰納的に，$K_{i+1} = E_{K_i}$ とおき，

$$\bar{K} = \bigcup_{0 \leq i < \infty} K_i$$

とおく．

作り方より，K_{i+1}/K_i は代数拡大で，任意の $f(x) \in K_i[x]^*$ は K_{i+1} に少なくとも1根をもつ．よって $\bar{K} = \bigcup_i K_i$ も K の代数拡大で，任意の $f(x) \in \bar{K}[x]^* = \bigcup_i K_i[x]^*$ は $\bar{K}$ 内に少なくとも1根をもつ．したがって，$\bar{K}$ は K の代数的閉包である．

（2）$\sigma : K_1 \xrightarrow{\sim} K_2$ を体の同型とする．そこで $\bar{K}_1/K_1$ の中間体 L と，L から $\bar{K}_2$ の中への同型 $\tau : L \longrightarrow \bar{K}_2$ で，σ の拡張であるものの組 (L, τ) の全体を $\mathscr{L}$ で表し，$\mathscr{L}$ に

$$(L_1, \tau_1) \leqq (L_2, \tau_2) \iff L_1 \subset L_2 \text{ かつ } \tau_2 \text{ は } \tau_1 \text{ の拡張}$$

という関係で順序を入れる．

$\{(L_\lambda, \tau_\lambda)\}_{\lambda \in \Lambda}$ が $\mathscr{L}$ の全順序部分集合なら，$L = \bigcup_\lambda L_\lambda$ も $\bar{K}_1/K_1$ の中間体である．そこで各 $\alpha \in L$ に対して任意に $\alpha \in L_\lambda$ なる λ を選び，

$$\tau(\alpha) = \tau_\lambda(\alpha)$$

とおく．このとき τ は L から $\bar{K}_2$ の中への体の同型で，$(L_\lambda, \tau_\lambda) \leqq (L, \tau)$ が任意の $\lambda \in \Lambda$ について成り立つ．よって $\mathscr{L}$ は帰納的順序集合となる．

そこで，ツォルンの補題を使い，$\mathscr{L}$ の極大元 (K_1^*, σ^*) をとる．もし $K_1^* \subsetneqq \bar{K}_1$ なら，$\alpha_1 \in \bar{K}_1 \setminus K_1^*$ をとり，α_1 の K_1^* 上の最小多項式を $f_1(x)$ で表す．また $\sigma^* : K_1^* \longrightarrow \bar{K}_2$ の像を K_2^* で表し，$f_2(x) = \sigma^*(f_1(x)) \in \bar{K}_2[x]$ とおき，$f_2(x)$ の $\bar{K}_2$ における1根を α_2 で表す．このとき，$f_1(x)$ は $K_1^*[x]$ で既約だから，$f_2(x)$ も $K_2^*[x]$ で既約となり，

$$\tau^* : \quad K_1^*(\alpha_1) \xrightarrow{\sim} K_1^*[x]/(f_1(x)) \xrightarrow{\sim} K_2^*[x]/(f_2(x)) \xrightarrow{\sim} K_2^*(\alpha_2)$$

なる同型ができる．これは (K_1^*, σ^*) の極大性に矛盾するから，$K_1^* = \bar{K}_1$ となる．

$\bar{K}_1$ は代数的閉体だから，$\mathrm{Im}(\sigma^*) \simeq K_1^* = \bar{K}_1$ も代数的閉体となる．$K_2 \subset \mathrm{Im}(\sigma^*) \subset \bar{K}_2$ であるから，$\mathrm{Im}(\sigma^*) = \bar{K}_2$ となり，$\bar{\sigma} = \sigma^*$ は $\bar{K}_1$ から $\bar{K}_2$ の上への同型となる．

（証明終）

系 2．9　Ω を代数的閉体，$\sigma: K \longrightarrow \Omega$ を Ω の中への体の同型，L/K を代数拡大とする．このとき σ は，$\tau: L \longrightarrow \Omega$ なる Ω の中への体の同型に拡張できる．

［**証 明**］　$K_1=K$，L の代数的閉包を $\bar{K}_1$，$\mathrm{Im}(\sigma)=K_2$，Ω における K_2 の代数的閉包を $\bar{K}_2$ とする．このとき定理より，$\sigma: K_1 \xrightarrow{\sim} K_2$ は $\bar{\sigma}: \bar{K}_1 \xrightarrow{\sim} \bar{K}_2 \subset \Omega$ なる同型に拡張できる．$\bar{\sigma}$ の L への制限を τ とおけばよい．　　（証明終）

K を体，$f(x) \in K[x]$ を定数でない多項式とする．このとき K の拡大体 L で，

$$L = K(\theta_1, \theta_2, \cdots, \theta_n),$$
$$f(x) = c(x-\theta_1)(x-\theta_2)\cdots(x-\theta_n) \qquad (c \in K)$$

となるものを $f(x)$ の（**最小**）**分解体** とよぶ．$\bar{K}$ を K の代数的閉包とし，$\bar{K}[x]$ で $f(x)$ を 1 次式の積に分解し，その根を $\theta_1, \theta_2, \cdots, \theta_n$，$L=K(\theta_1, \theta_2, \cdots, \theta_n)$ とおくと，L は $f(x)$ の分解体となる．

次に $L'=K(\theta_1', \theta_2', \cdots, \theta_n')$ も $f(x)$ の分解体であるとする．このとき L'/K は代数的だから，系 2.9 により，K-同型 $\tau: L' \longrightarrow \bar{K}$ が存在する．しかも

$$\tau(L') = K(\tau(\theta_1'), \tau(\theta_2'), \cdots, \tau(\theta_n')),$$
$$f(x) = c(x-\tau(\theta_1'))(x-\tau(\theta_2'))\cdots(x-\tau(\theta_n'))$$

となるから，$\{\tau(\theta_1'), \tau(\theta_2'), \cdots, \tau(\theta_n')\}$ は $\{\theta_1, \theta_2, \cdots, \theta_n\}$ と集合として一致する．よって，τ は L' から L への K-同型となる．したがって，

命 題 2．10　$f(x) \in K[x]$ が定数でないとき，$f(x)$ の分解体は存在し，K-同型の差を除き一意的に定まる．

例 2．11　$K=\boldsymbol{Q}$，$f(x)=x^3-5$，$\omega=(-1+\sqrt{-3})/2$ とおくと，$\boldsymbol{Q}(\sqrt[3]{5})$，$\boldsymbol{Q}(\omega\sqrt[3]{5})$，$\boldsymbol{Q}(\omega^2\sqrt[3]{5})$ は $f(x)$ の根体，$\boldsymbol{Q}(\sqrt{-3}, \sqrt[3]{5})$ は $f(x)$ の分解体となる．

問 題 2．12　$\bar{K}$ を K の代数的閉包とし，α, β を $\bar{K}$ の元とする．このとき，次は同値であることを示せ．

（1） α, β の K 上の最小多項式は一致する．

（2） $\sigma : K(\alpha) \longrightarrow K(\beta)$ なる K-同型で，$\sigma(\alpha) = \beta$ となるものが存在する．

（3） $\sigma : \bar{K} \longrightarrow \bar{K}$ なる K-同型で，$\sigma(\alpha) = \beta$ となるものが存在する．

この条件が満たされるとき，$\alpha, \beta \in \bar{K}$ は K 上で **共役** であるという．

§3. 正 規 拡 大

以下，$\sigma : K \longrightarrow K'$ を体の同型，$a \in K$，$S \subset K$ とするとき，像 $\sigma(a)$ や $\sigma(S)$ のことを，慣例に従って a^σ や S^σ とも表す．この場合，$a^{\sigma\tau}$ は $(a^\sigma)^\tau$ のことと理解すると，

$$a^{\sigma\tau} = (a^\sigma)^\tau = \tau(a^\sigma) = \tau(\sigma(a)) = (\tau\sigma)(a)$$

となり，写像としての合成とは，積の順序が逆になる．本書では，混乱をさけるため，a^σ や S^σ という書き方は使うが，$a^{\sigma\tau}$ や $S^{\sigma\tau}$ は使わない．

3.1 正規拡大　まず次の命題を示す．

命題 3.1　代数拡大 L/K において，次は同値である．

（1） L の任意の拡大体 N に対し，N/K の中間体で L と K-同型なものは L に限る．

（2） L の代数的閉包は K の代数的閉包にもなるから，それを $\bar{K}$ で表す．このとき，$\bar{K}$ の任意の K-同型 σ に対し，$L^\sigma = L$ が成り立つ．

（3） 既約多項式 $f(x) \in K[x]$ が L において根をもてば，$f(x)$ は L で 1 次式の積に分解される．

以下，この命題 (1)～(3) のどれかが成り立つとき，代数拡大 L/K は **正規** であるという．

[**証明**] (1) $\Longrightarrow$ (2)．$\sigma : \bar{K} \longrightarrow \bar{K}$ を K-同型とすると，L^σ は L と K-同型になる．よって仮定より，$L^\sigma = L$ が成り立つ．

(2) $\Longrightarrow$ (3)．$f(x) \in K[x]$ を L に根をもつ既約多項式とし，その根を θ で表す．このとき，$f(x)$ は $\bar{K}[x]$ において，

$$f(x) = c(x-\theta_1)(x-\theta_2)\cdots(x-\theta_n) \qquad (\theta_1 = \theta,\ c \in K)$$

と1次式の積に分解される．ここで $K(\theta_i)$ は $f(x)$ の根体をなすから，命題1.6（根体の一意性）より，

$$\sigma_i: \quad K(\theta) \stackrel{\sim}{\to} K(\theta_i)$$

なる K–同型が存在する．この σ_i は，定理2.8より，$\bar{\sigma}_i: \bar{K} \longrightarrow \bar{K}$ なる K–同型に拡張できる．ところが仮定より，$\sigma_i(L) = L$ が成り立つから，$\theta_i = \sigma_i(\theta) \in \sigma_i(L) = L$ となる．よって，すべての根 θ_i が L に入るから，$f(x)$ は $L[x]$ で1次式の積となる．

（3）$\Longrightarrow$（1）．$N \supset L, L' \supset K$ とし，$\sigma: L \longrightarrow L'$ が K–同型であるとする．L の任意の元 θ に対し，その最小多項式を $L[x]$ で分解すると，仮定より，

$$\mathrm{Irr}(\theta, K, x) = (x-\theta_1)(x-\theta_2)\cdots(x-\theta_n) \qquad (\theta_1 = \theta,\ \theta_i \in L)$$

の形となる．この左辺を σ で動かしても，$\mathrm{Irr}(\theta, K, x) \in K[x]$ は動かない．他方，右辺を σ で動かすと，$(x-\theta_1{}^{\sigma})(x-\theta_2{}^{\sigma})\cdots(x-\theta_n{}^{\sigma})$ となる．よって，$\theta^{\sigma} = \theta_1{}^{\sigma}$ は $\mathrm{Irr}(\theta, K, x)$ の根だから，$\theta_1, \theta_2, \cdots, \theta_n$ のどれかと一致し，L に入る．よって $L \supset L^{\sigma} = L'$ となる．$\sigma^{-1}: L' \longrightarrow L$ についても同じことを行うと，$L \subset L'$ となり，$L = L'$ を得る．（証明終）

命題の（2）を使うと，次の系を得る．

系 3．2 N/K を体の拡大とし，その中間体 L_1, L_2 が共に K 上正規であるとする．このとき，$L_1 \cap L_2$ と $L_1 \cdot L_2$ も K 上正規な拡大となる．

また，定理2.8（シュタイニッツの定理）の（2）と，命題3.2の（2）より，次の系が得られる．

系 3．3 $\bar{K}$ を体 K の代数的閉包とし，$\bar{K} \supset N \supset L \supset K$ を中間体の列で，N/K が正規拡大であるとする．このとき，$\sigma: L \longrightarrow \bar{K}$ なる L から $\bar{K}$ の中への K–同型は，$\bar{\sigma}(N) = N$ なる $\bar{K}$ の K–自己同型 $\bar{\sigma}$ に拡張される．

問題 3．4 系3.3の条件のもとで，$\alpha, \beta \in L$ が K 上共役となるための必要十分条件は，$\alpha^{\tau} = \beta$ なる N の K–自己同型 τ が存在することであることを示せ．

3．2 正規拡大の特徴づけ 次の定理は，有限次の正規拡大の特徴づけを与える．

定 理 3. 5 有限次拡大 L/K が正規拡大となるための必要十分条件は，L がある多項式 $f(x) \in K[x]$ の分解体となることである．

[証 明] (必要性) L/K は有限次拡大だから，定理 2.1 により，$L = K(\theta_1, \theta_2, \cdots, \theta_n)$ と有限生成な代数拡大となる．そこで $f_i(x) = \mathrm{Irr}(\theta_i, K, x)$ とおき，その積を $f(x)$ で表す．L/K は仮定より正規だから，各 $f_i(x)$ は $L[x]$ で 1 次式の積に分解し，$f(x) = \prod_i f_i(x)$ の根はすべて L に属す．ところが，L は $f(x)$ の根である $\theta_1, \theta_2, \cdots, \theta_n$ により K 上生成されるから，L は $f(x)$ の K 上の分解体となる．

(十分性) L が $f(x) \in K[x]$ の分解体であるものとし，$\bar{K}$ を L を含む K の代数的閉包とする．$\sigma : \bar{K} \longrightarrow \bar{K}$ を K-同型とすると，σ は K の元を動かさず，したがって $f(x) \in K[x]$ も動かさない．よって $f(x) = \prod_{i=1}^{n} (x - \theta_i)$ とすると，$\{\theta_1{}^\sigma, \theta_2{}^\sigma, \cdots, \theta_n{}^\sigma\} = \{\theta_1, \theta_2, \cdots, \theta_n\}$ となり，$L^\sigma = K(\theta_1{}^\sigma, \theta_2{}^\sigma, \cdots, \theta_n{}^\sigma) = K(\theta_1, \theta_2, \cdots, \theta_n) = L$ が成り立つ．よって，命題 3.1，(2) より，L/K は正規拡大である． (証明終)

系 3. 6 L/K を有限次拡大とし，$\bar{K}$ を L の代数的閉包とする．このとき，$\bar{K} \supset N \supset L$ なる K の有限次の正規拡大 N が存在する．

[証 明] $L = K(\theta_1, \theta_2, \cdots, \theta_n)$，$f_i(x) = \mathrm{Irr}(\theta_i, K, x)$，$f(x) = f_1(x) f_2(x) \cdots f_n(x)$ とし，$f(x)$ の分解体を N とおけばよい． (証明終)

§4. 分 離 性

4. 1 正標数の体 K を標数 $p > 0$ の体とする．したがって，p は素数で，K の任意の元 a に対し，$p \cdot a = 0$ となるものとする（例 1.1 参照）．このとき二項係数

$$\binom{p}{i} = \frac{p!}{i!\,(p-i)!} = \frac{(i+1)\cdot(i+2)\cdots(p-1)\cdot p}{1\cdot 2\cdots(p-i-1)\cdot(p-i)} \qquad (1 \leqq i \leqq p-1)$$

は，p で割り切れる．したがって，$b, c \in K$ のとき，

$$(b+c)^p = \sum_{0 \leqq i \leqq p} \binom{p}{i} b^i c^{p-i} = b^p + c^p$$

が成り立つ.

e を自然数, $q = p^e$ とし, F_q で

$$F_q: \quad K \ni a \longmapsto a^q \in K$$

なる写像を表す. $(b+c)^{p^e} = \{(b+c)^{p^{e-1}}\}^p = (b^{p^{e-1}} + c^{p^{e-1}})^p = b^{p^e} + c^{p^e}$ だから, F_q は K の加法群の準同型である. また $(bc)^q = b^q c^q$ も成り立つから, F_q は K から K の中への体の同型である. とくに F_q は単射である (179 ページ参照). これを K の q 乗 **フロベニウス写像** とよぶ.

例 4. 1 K を標数 $p>0$ の体, $q = p^e$ $(e \in N)$, $a \in K$ とし, K の代数的閉包の中での $x^q = a$ の 1 根を $a^{1/q}$ で表す. このとき

$$x^q - a = (x - a^{1/q})^q$$

が成り立つ. したがって, $x^q = a$ の根は唯一つしかない. 同様にして, $f(x) \in K[x]$ の根を重複度も含め $\theta_1, \theta_2, \cdots, \theta_n$ とすると, $f(x^q)$ の根は, ${\theta_1}^{1/q}, {\theta_2}^{1/q}, \cdots, {\theta_n}^{1/q}$ が q 回重複して現れることもわかる.

4. 2 多項式の分離性

K を体, $f(x) \in K[x]$ のとき,

$$f'(x) = \lim_{h\to 0} \frac{1}{h} \{f(x+h) - f(x)\}$$

とおき, $f(x)$ の **微分** とよぶ. ($1/h$ 以下は, x と h の多項式である.)

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0$$

のとき, 二項展開を使うと, その微分は

$$f'(x) = n a_n x^{n-1} + (n-1) a_{n-1} x^{n-2} + \cdots + 2a_2 x + a_1$$

で与えられることがわかる. また通常の場合と同様にして,

$$\{f(x)g(x)\}' = f'(x)g(x) + f(x)g'(x)$$

$$\{f(g(x))\}' = f'(g(x))g'(x)$$

等の公式が成り立つこともわかる.

$f(x) \in K[x]$ を定数でない多項式とし, K の代数的閉包 $\bar{K}$ において,

$$f(x) = c(x-\theta_1)^{m_1}(x-\theta_2)^{m_2}\cdots(x-\theta_n)^{m_n}$$

と相異なる 1 次式の積に分解する. このとき, ある i について $m_i \geqq 2$ となる

なら，$f(x)$ は**重根** θ_i をもつといい，また $f(x)$ は**非分離的**であるという．逆に $f(x)$ が重根をもたないなら，$f(x)$ は**分離的**であるという．

θ を $f(x)$ の1根とし，

$$f(x) = (x-\theta)^m g(x) \qquad (g(x) \in \bar{K}[x],\ g(\theta) \neq 0)$$

と書く．これを微分すると，

$$f'(x) = m(x-\theta)^{m-1} g(x) + (x-\theta)^m g'(x)$$

となるから，$m \geqq 2$ となるための必要十分条件は $f'(\theta) = 0$ となることである．つまり，$f(x)$ が非分離的となるための必要十分条件は，$f(x)$ と $f'(x)$ が共通根をもつことである．これを使うと次の定理が得られる．

定理 4.2 (1) K を標数0の体とすると，任意の既約多項式 $f(x) \in K[x]$ は分離的である．

(2) K の標数を $p > 0$ とし，$f(x) \in K[x]$ が既約であるとする．このとき，分離的な既約多項式 $f_s(x) \in K[x]$ と自然数 e があり，

$$f(x) = f_s(x^q) \qquad (q = p^e)$$

と書ける．

[証明] $f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0 \in K[x]$ $(a_n \neq 0)$ を既約多項式だとする．このとき，

$$f'(x) = n a_n x^{n-1} + (n-1) a_{n-1} x^{n-2} + \cdots + 2a_2 x + a_1$$

である．よって $\deg f'(x) < \deg f(x)$ である．そこで，もし $f(x)$ が重根 θ をもつなら，θ は $f'(x)$ の根ともなり，$f(x)$ は θ の最小多項式の a_n 倍だから，$f'(x) \equiv 0$ となる．よって

$$na_n = 0, \quad (n-1)a_{n-1} = 0, \quad \cdots, \quad 2a_2 = 0, \quad a_1 = 0$$

となる．

もし K の標数が0なら，$a_n \neq 0$ より $n \cdot a_n \neq 0$ となり矛盾する．よって，(1) が成り立つ．したがって，K の標数は $p > 0$ であるとする．このとき，

$$ia_i = 0 \iff i \equiv 0 \pmod p \text{ または } a_i = 0$$

である．よって $n = pn_1$ $(n_1 \in \boldsymbol{N})$ と書け，

$$f(x) = a_n x^{pn_1} + a_{n-p} x^{p(n_1-1)} + \cdots + a_p x^p + a_0$$

の形となる．したがって，

$$f(x) = f_1(x^p) \qquad (f_1(x) \in K[x])$$

と書ける．もし $f_1(x)$ も重根をもつなら，$f_1(x)$ についても同じことができる．ところが，$\deg f_1(x) < \deg f(x)$ だから，この操作は有限回で終り，ある重根をもたない多項式 $f_s(x) \in K[x]$ と $e \geqq 1$ があり，

$$f(x) = f_s(x^q) \qquad (q = p^e)$$

と書ける．$f(x)$ は既約だから，$f_s(x)$ も既約となり，定理は証明された．

(証明終)

K を標数が $p > 0$ の体とし，$f(x) \in K[x]$ を既約多項式とする．このとき，定理のような $f_s(x)$ と e をとり，$f_s(x)$, $\deg f_s$, p^e, e をそれぞれ **被約多項式，被約次数，非分離次数，非分離指数** とよぶ．そこで $\deg_s f = \deg f_s$, $\deg_i f = p^e$ とおく．明らかに

$$\deg f = \deg_s f \cdot \deg_i f$$

が成り立つ．とくに $\deg_s f = 1$ のとき，$f(x)$ を **純非分離的** であるという．

K の標数が 0 のときは，任意の既約多項式は分離的となるので，$f_s(x) = f(x)$, $e = 0$, $p^e = 1$, $\deg_s f = \deg f$, $\deg_i f = 1$ と思う．そうすると，標数が 0 のときも同じ記号が使える．

θ を体 K 上代数的な元とする．このとき，$f(x) = \mathrm{Irr}(\theta, K, x)$ とおき，$f(x)$ が分離的または非分離的のとき，θ を K 上 **分離的** である，または **非分離的** であるという．θ の **被約次数，非分離次数** なども，$f(x)$ のそれらを使って定義する．

L/K を代数拡大とする．このとき，任意の $\theta \in L$ が K 上分離的なら，拡大 L/K は **分離的** だといい，そうでないとき L/K は **非分離的** だという．また，K の代数的閉包を $\bar{K}$ とするとき，L の $\bar{K}$ の中への K-同型の個数を $[L:K]_s$ で表し，L/K の **分離次数** とよぶ．とくに $[L:K]_s = 1$ のとき，L/K は **純非分離的** であるという．これらの定義が妥当なことは，4.3 (定理 4.4) で示す．

4. 3 同型の拡張と分離性　まず次の補題を示す．

補 題 4. 3　L/K を代数拡大とし，M をその中間体とする．このとき，

$$[L:K]_s=[L:M]_s[M:K]_s$$

が成り立つ．

［証 明］　$\bar{K}$ を L を含む K の代数的閉包とし，$\sigma_i: M \longrightarrow \bar{K}$ $(i \in I)$ を（$\bar{K}$ の中への）相異なる K-同型の全体，$\tau_j: L \longrightarrow \bar{K}$ $(j \in J)$ を相異なる M-同型の全体とする．定理2.8の（2）を使い，σ_i を $\bar{\sigma}_i: \bar{K} \longrightarrow \bar{K}$ なる同型に拡張し，$\rho_{ij}: L \longrightarrow \bar{K}$ を $\rho_{ij}=\bar{\sigma}_i \circ \tau_j$ として定める．ρ_{ij} の M への制限は σ_i と一致するから，$\{\rho_{ij}\}_{ij}$ は i が異なれば異なる．また $\bar{\sigma}_i \circ \tau_{j_1}=\bar{\sigma}_i \circ \tau_{j_2}$ より $\tau_{j_1}=\tau_{j_2}$ が導かれるから，$\{\rho_{ij}\}_{ij}$ はすべて相異なる．

$\rho: L \longrightarrow \bar{K}$ を任意の（$\bar{K}$ の中への）K-同型とする．このとき ρ の M への制限はある σ_i に一致し，したがって，$(\bar{\sigma}_i)^{-1} \circ \rho: L \longrightarrow \bar{K}$ は M 上自明となる．よって $(\bar{\sigma}_i)^{-1} \circ \rho$ はある τ_j と一致し，$\rho=\bar{\sigma}_i \circ \tau_j=\rho_{ij}$ が成り立つ．したがって，このような ρ の個数 $[L:K]_s$ は $\#(I)\#(J)=[M:K]_s[L:M]_s$ に等しい．　（証明終）

定 理 4. 4　L/K を有限次拡大とする．このとき，

（1）　$$[L:K]=[L:K]_s p^e$$

と書ける．ここで p は K の標数，e は非負整数とし，K の標数が0なら $p^e=1$ とみなす．とくに $[L:K]_s \leqq [L:K]$ が成り立つ．

（2）　L/K が分離的となるための必要十分条件は，$[L:K]_s=[L:K]$ が成り立つことである．

（3）　Ω を代数的閉体とし，$\sigma: K \longrightarrow \Omega$ を Ω の中への体の同型とする．このとき，$\tau: L \longrightarrow \Omega$ なる同型で σ の拡張となるものの個数は，$[L:K]_s$ に等しい．

［証 明］　まず L/K が単拡大の場合に，(1)，(3) が成り立つことを示す．

$L=K(\theta)$，$f(x)=\mathrm{Irr}(\theta,K,x)$ とし，$f(x)=f_s(x^q)$ $(q=p^e)$ を定理4.2のようにとる．K の L を含む代数的閉包を $\bar{K}$ とし，$\bar{K}[x]$ において

$$\mathrm{Irr}(\theta,K,x)=f_s(x^q)=\{(x-\theta_1)(x-\theta_2)\cdots(x-\theta_n)\}^q$$

$(\theta_i \in \bar{K})$ と表す．

$\sigma: K \longrightarrow \Omega$ を同型とし，$\tau: L \longrightarrow \Omega$ をその拡張とする．τ を何か $\bar{\sigma}: \bar{K} \longrightarrow \Omega$ な

る同型に拡張し，上式を $\bar{\sigma}$ で移すと

$$\mathrm{Irr}(\theta, K, x)^{\sigma} = \mathrm{Irr}(\tau(\theta), \sigma(K), x) = \{(x-\bar{\sigma}(\theta_1))(x-\bar{\sigma}(\theta_2))\cdots(x-\bar{\sigma}(\theta_n))\}^q$$

となる．したがって，$\tau(\theta) = \bar{\sigma}(\theta_i)$ $(1 \leqq i \leqq n)$ となる．ところが逆に，$\sigma : K \longrightarrow \Omega$ は $\tau(\theta) = \bar{\sigma}(\theta_i)$ を満たす同型 $\tau : L \longrightarrow \Omega$ に拡張できるから，

$$\sharp\{\tau : K(\theta) \longrightarrow \Omega \mid \sigma \text{ の拡張}\} = n = \deg f_s$$

が成り立つ．

$\Omega = \bar{K}$，$\sigma = \mathrm{id}_K$ としてこの式を使うと，

$$[K(\theta) : K]_s = \deg f_s < \infty$$

が得られる．したがって，

$$\sharp\{\tau : K(\theta) \longrightarrow \Omega \mid \sigma \text{ の拡張}\} = [K(\theta) : K]_s$$

であるから，(3) が成り立つ．また

$$[K(\theta) : K] = \deg f(x) = \deg f_s(x)\, q = [K(\theta) : K]_s\, q \qquad (q = p^e)$$

であるから，(1) も成り立つ．さらに，単拡大 $K(\theta)/K$ において θ が K 上分離的なら，$q=1$ となるから，$[K(\theta) : K] = [K(\theta) : K]_s$ も成り立つ．

次に L/K が単拡大でないものとし，$L \supsetneqq M \supsetneqq K$ なる中間体 M をとり，(1)，(3) を示す．この場合，L/K の生成元の個数に関する帰納法により，L/M，M/K においては (1)，(3) が成り立つとしてよい．したがって，$\sigma : K \longrightarrow \Omega$ は $[M : K]_s$ 個の $\rho : M \longrightarrow \Omega$ に拡張でき，各 $\rho : M \longrightarrow \Omega$ は $[L : M]_s$ 個の $\tau : L \longrightarrow \Omega$ に拡張できるとする．このとき，命題 1.2 と補題 4.3 より

$$[L : K] = [L : M][M : K], \qquad [L : K]_s = [L : M]_s[M : K]_s$$

が成り立つから，定理の (1)，(3) が一般に成り立つ．

最後に (2) を示す．

L/K が有限次分離拡大だとし，$L = K(\theta_1, \theta_2, \cdots, \theta_n)$ とする．$L_0 = K$，$L_i = K(\theta_1, \theta_2, \cdots, \theta_i)$ とおくと，$L_i = L_{i-1}(\theta_i)$ となる．θ_i は K 上分離的だから，$\mathrm{Irr}(\theta_i, K, x)$ は重根をもたず，したがって，その一部である $\mathrm{Irr}(\theta, L_{i-1}, x)$ も，重根をもたない．よって θ_i は L_{i-1} 上分離的となり，$[L_i : L_{i-1}]_s = [L_i : L_{i-1}]$ が成り立つ．したがって，

$$\begin{aligned}[L : K]_s &= [L_n : L_{n-1}]_s[L_{n-1} : L_{n-2}]_s \cdots [L_1 : L_0]_s \\ &= [L_n : L_{n-1}][L_{n-1} : L_{n-2}] \cdots [L_1 : L_0] = [L : K]\end{aligned}$$

が成り立つ．

逆に，有限次拡大 L/K において $[L : K]_s = [L : K]$ が成り立つとする．$\theta \in L$ を任

意にとり，$M = K(\theta)$ とおくと，

$$[L:M]_s[M:K]_s = [L:K]_s = [L:K] = [L:M][M:K]$$

が成り立つ．また（1）より，

$$[L:M]_s \leqq [L:M], \qquad [M:K]_s \leqq [M:K]$$

が成り立つから，$[L:M]_s = [L:M]$，$[M:K]_s = [M:K]$ となる．M/K は単拡大だから，この定理の証明の最初の部分により，$\mathrm{Irr}(\theta, K, x)$ が $[M:K]_s = [M:K] = [K(\theta):K]$ 個の相異なる根をもつことがわかる．したがって，θ は K 上分離的となる．これで定理の証明は完成した． (証明終)

定理 4.4 による分離拡大の特徴づけを使うと，いろいろなことがわかる．

命題 4.5 （1） L/K を代数拡大とし，M をその中間体とする．このとき L/K が分離的となるための必要十分条件は，L/M および M/K が分離的なことである．

（2） L/K を代数拡大とし，$S \subset L$ とする．このとき，S の任意の元が K 上分離的なら，$K(S)$ は K 上分離的である．

［証 明］ （1） L/K が分離的なら，任意の $\theta \in L$ について $\mathrm{Irr}(\theta, K, x)$ が重根をもたない．このとき，任意の $\theta \in M$ に対し，$\mathrm{Irr}(\theta, K, x)$ は重根をもたない．また任意の $\theta \in L$ に対し，$\mathrm{Irr}(\theta, M, x)$ は $\mathrm{Irr}(\theta, K, x)$ を割り切るから，これも重根をもたない．これは M/K および L/M が分離的なことを意味する．

逆に M/K，L/M が分離的だとし，$\theta \in L$ の M 上の最小多項式を

$$\mathrm{Irr}(\theta, M, x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \qquad (a_i \in M)$$

とおく．このとき，$N = K(a_{n-1}, \cdots, a_1, a_0)$ は M の部分体だから，K 上分離的である．また $\mathrm{Irr}(\theta, N, x) = \mathrm{Irr}(\theta, M, x)$ だから，$N(\theta)/N$ も分離的である．ところが $N(\theta)/K$ は有限次拡大だから，補題 4.3 と定理 4.4 より，

$$[N(\theta):K]_s = [N(\theta):N]_s[N:K]_s = [N(\theta):N][N:K] = [N(\theta):K]$$

が成り立つ．したがって，定理 4.4 より，$N(\theta)/K$ は分離的である．

（2） $\theta \in K(S)$ に対し，適当な S の有限部分集合 $F = \{\theta_1, \theta_2, \cdots, \theta_n\}$ で $\theta \in K(F)$ なるものをとり，$L_i = K(\theta_1, \theta_2, \cdots, \theta_i)$ とおく．θ_i は K 上分離的だから，L_{i-1} 上でも分離的である．ところが $L_i = L_{i-1}(\theta_i)$ は単拡大だから，定理 4.4 の証明より，$[L_i : L_{i-1}]_s$

$=[L_i:L_{i-1}]$ が成り立つ．よって

$$[K(F):K]_s=[L_n:L_{n-1}]_s[L_{n-1}:L_{n-2}]_s\cdots[L_1:K]_s$$
$$=[L_n:L_{n-1}][L_{n-1}:L_{n-2}]\cdots[L_1:K]=[K(F):K]$$

が成り立ち，$K(F)/K$ は分離的である．したがって，任意の $\theta\in K(F)$ は K 上分離的である． (証明終)

系 4.6 (1) L/K を分離的だとする．このとき，任意の拡大 M/K に対し，合成体 $L\cdot M$ は M 上分離的である．

(2) L_1, L_2 を K の分離拡大とする．このとき，合成体 $L_1\cdot L_2$ も K 上分離的である．

(3) L/K を代数拡大とし，K 上分離的な L の元全体のなす集合を L_s で表す．このとき L_s は体をなし，L/L_s は純非分離拡大となる．この L_s を，K の L における **分離閉包** という．

[証明] $L\cdot M=M(L)$，$L_1\cdot L_2=L_1(L_2)$ だから，(1)，(2) は命題の (2) より明らかである．(3) についても，L_s が体をなすことは，命題の (2) より明らかである．もし L/L_s が純非分離的でないなら，$\sigma: L\longrightarrow\bar{L}$ なる L_s–同型で，id_L でないものが存在する．そこで，$\theta\in L$ で $\sigma(\theta)\neq\theta$ なるものをとると，$[L_s(\theta):L_s]_s\neq 1$ となる．したがって，定理 4.2 と定理 4.4 より，適当な自然数 e をとると，$\theta_1=\theta^{p^e}$ は L_s 上分離的で $[L_s(\theta_1):L_s]=[L_s(\theta):L_s]_s\neq 1$ となる．ところが L_s/K は分離的だから，θ_1 は K 上でも分離的となり，これは L_s の定義に矛盾する． (証明終)

例 4.7 $\bar{K}$ を K の代数的閉包とする．このとき，$\theta\in\bar{K}$ が K 上純非分離的なら，適当な整数 $e\geqq 0$ をとると，$\mathrm{Irr}(\theta,K,x)=x^{p^e}-a$ $(a\in K)$ となる．したがって，θ は

$$K^{p^{-e}}=\{\theta\in\bar{K}\mid\theta^{p^e}\in K\}$$

の元となる．また $\theta^{p^{e-1}}\in K^{p^{-1}}$, $\notin K$ だから，次の (1)〜(3) は同値である：

(1) K 上の代数的な元はすべて分離的である．

(2) $K^{p^{-1}}=K$.

(3) $F_p: K\ni a\longmapsto a^p\in K$ が全射である．

この性質を K がもつとき，K は **完全体** であるという．F_p は単射であるから，K が有限体なら全射にもなる．よって有限体は完全体である．系 4.6, (3) より，完全体の任

意の代数拡大は分離拡大となる．

例 4. 8　L/K を分離拡大とし，$\bar{K}$ を L の代数的閉包とする．L/K は分離的だから，任意の $\theta \in L$ の $\mathrm{Irr}(\theta, K, x)$ は重根をもたない．したがって，$\mathrm{Irr}(\theta, K, x)$ の根である θ の K 上の共役元（問題 2. 12 参照）も K 上分離的である．そこで，θ を L の元を動かしたとき，θ の K 上の共役元全体で生成される K の分離拡大を L_1 とする．これは $\bar{K}/K$ の自己同型で不変だから，L_1/K は正規拡大である．定義より明らかに，L_1 は L を含む最小の正規拡大である．また，L/K が有限次拡大なら，L_1/K も有限次拡大となる．
L_1/K を L/K の **ガロア閉包** とよぶ（202 ページ参照）．

4. 4　有限次分離拡大

定 理 4. 9　$L = K(\theta_1, \theta_2, \cdots, \theta_n)$ を K の有限次拡大とし，$\theta_2, \cdots, \theta_n$ が K 上分離的だとする．このとき適当な $\theta \in L$ をとると，$L = K(\theta)$ となる．とくに，有限次の分離拡大は単拡大となる．

［**証 明**］　有限体の乗法群は巡回群となることを §6 で示すから，K が有限体なら，L の乗法群の生成元を θ とすればよい．よって，以下 K は無限体だとする．

帰納法により $n = 2$ の場合に示せばよいから，$L = K(\alpha, \beta)$ で，β が K 上分離的だとする．$\sigma_1, \sigma_2, \cdots, \sigma_m$ を相異なる L の $\bar{K}$ への K 上のうめ込みの全体とする．$i \neq j$ なら，$\sigma_i(\alpha) \neq \sigma_j(\alpha)$ または $\sigma_i(\beta) \neq \sigma_j(\beta)$ である．したがって，

$$f(x) = \prod_{i \neq j} \{(\sigma_i(\alpha) - \sigma_j(\alpha))x + (\sigma_i(\beta) - \sigma_j(\beta))\} \in \bar{K}[x]$$

は 0 以外の多項式である．K は無限体だから，K は $cf(c) \neq 0$ なる元 c を含む．そこで

$$\theta = \alpha c + \beta \in L$$

とおくと，$\sigma_i(\theta) \neq \sigma_j(\theta)$ $(i \neq j)$ が成り立つ．したがって，

$$[K(\theta) : K]_s \geqq m = [L : K]_s = [L_s : K]$$

が成り立つから，$K(\theta)$ は K の L における分離閉包 L_s を含む．よって $\beta \in K(\theta)$ となる．ところが，

$$\alpha = c^{-1}(\theta - \beta) \in K(\theta, \beta) = K(\theta)$$

であるから，$L = K(\alpha, \beta) = K(\theta)$　となる．　　（証明終）

問 題 4. 10　k を標数 $p > 0$ の体とし，k 上の 2 変数の有理関数のなす体を $L = k(x,$

y), $K = k(x^p, y^p)$ とおく．このとき，L/K は単拡大とはならないことを示せ．
（ヒント：$\forall\theta \in L$ に対し，$\theta^p \in K$ となる．）

§5. ガロア拡大

5.1 ガロア拡大 体 L から体 L の上への同型全体のなす群を $\mathrm{Aut}(L)$ と表し，K を L の部分体とするとき，L から L の上への K-同型全体のなす群を $\mathrm{Aut}(L/K)$ と表した．

L を体とし，G を $\mathrm{Aut}(L)$ の部分群とする．このとき

$$F(G) = \{a \in L \mid a^\sigma = a \ \ (\sigma \in G)\}$$

とおき，G の **不変体**（または **固定体**）とよぶ．明らかに，

$$G_1 \subset G_2 \implies F(G_1) \supset F(G_2)$$

が成り立つ．

代数拡大 L/K が正規かつ分離的となるとき，L/K は **ガロア拡大** であるという．このとき

$$\mathrm{Gal}(L/K) = \mathrm{Aut}(L/K) = \{\sigma : L \simeq L \mid K\text{-同型}\}$$

とおき，これを L/K の **ガロア群** とよぶ．とくにこの群 $\mathrm{Gal}(L/K)$ が巡回群，アーベル群，可解群となるとき，対応するガロア拡大 L/K を **巡回拡大**，**アーベル拡大**，**可解拡大** などとよぶ．

（注） $\mathrm{Gal}(L/K)$ のことを，$G(L/K)$ と書くことも多い．

L/K をガロア拡大とし，M をその中間体とする．このとき，L は M 上でも正規かつ分離的となる．よって L/M もガロア拡大となり，そのガロア群 $\mathrm{Gal}(L/M)$ は $\mathrm{Gal}(L/K)$ の部分群となる．これを中間体 M に対する **不変群** とよぶ．M_1, M_2 を L/K の中間体とすると，

$$M_1 \supset M_2 \implies \mathrm{Gal}(L/M_1) \subset \mathrm{Gal}(L/M_2)$$

が成り立つ．

定義より明らかに，F と G の間には

$$\mathrm{Aut}(L/F(G)) \supset G, \qquad F(\mathrm{Aut}(L/K)) \supset K$$

なる関係が成り立つ．このうち $\mathrm{Aut}(L/F(G)) \supset G$ なる関係は，一般には等号とはならないが，G が有限群なら等しくなる．また $F(\mathrm{Aut}(L/K)) \supset K$ の方は，任意のガロア拡大で等号が成り立つ．より詳しく，次の定理が成り立つ．

定理 5.1 (1) L/K を代数拡大とする．このとき，L/K がガロア拡大となるための必要十分条件は，K が $\mathrm{Aut}(L/K)$ の不変体となることである．

(2) (アルティン) G を体 L の自己同型の群 $\mathrm{Aut}(L)$ の有限部分群とし，$K = F(G)$ とおく．このとき，L/K は有限次ガロア拡大で，$\mathrm{Gal}(L/K) = G$，$[L:K] = \# G$ となる．

[証明] (1) L/K を代数拡大とし，$K = F(\mathrm{Aut}(L/K))$ が成り立つものとする．$G = \mathrm{Aut}(L/K)$ とおく．L/K は代数拡大だから，L の任意の元 θ は，有限個しか K 上の共役元をもたない．そこでそれらのうち L に入るもの全体を選び，$\theta_1 = \theta, \theta_2, \cdots, \theta_n$ とおく．明らかに $\sigma \in G$ はこれらを全体として保つから，$\{\sigma(\theta_1), \sigma(\theta_2), \cdots, \sigma(\theta_n)\} = \{\theta_1, \theta_2, \cdots, \theta_n\}$ となる．そこで $f(x) = \prod_{1 \leq i \leq n} (x - \theta_i)$ とおく．$f(x) \in L[x]$ の係数を σ で動かしたものを $f^{\sigma}(x) \in L[x]$ とする．このとき，任意の $\sigma \in G$ に対し，

$$f^{\sigma}(x) = \prod_i (x - \sigma(\theta_i)) = \prod_i (x - \theta_i) = f(x)$$

が成り立つから，$f(x)$ の係数は $K = F(G)$ に入る．

$f(x) \in K[x]$ は θ を根にもち，その根はすべて相異なる．よって，θ は K 上分離的となる．また θ の任意の K 上の共役元は，$f(x) \in K[x]$ の根となり，$\theta_1, \theta_2, \cdots, \theta_n \in L$ のどれかと一致する．よって L は，任意の $\theta \in L$ のすべての K 上の共役元を含むから，L/K は正規拡大となる．したがって，L/K はガロア拡大となる．

逆に，L/K がガロア拡大となるものとし，$G = \mathrm{Gal}(L/K)$ とおく．$\theta \in L$, $\theta \notin K$ なる元をとり，その最小多項式を $f(x)$ とおく．L/K は分離的だから，$f(x)$ は θ 以外の根 θ' をもつ．このとき，$K(\theta)$, $K(\theta')$ は $f(x)$ の根体となるから，$\sigma_0 : K(\theta) \longrightarrow K(\theta')$ なる K-同型で，$\sigma_0(\theta) = \theta'$ なるものが存在する．この σ_0 を，K の L を含む代数的閉包の自己同型 $\tilde{\sigma}$ に拡張し，$\tilde{\sigma}$ の L への制限を σ とおく．L/K は正規だから，$\sigma(L) = L$ である．したがって，$\sigma \in \mathrm{Gal}(L/K)$ で $\sigma(\theta) = \theta'$ なるものが存在する．$\sigma(\theta) = \theta' \neq \theta$ だから，これは $\theta \notin F(G)$ を意味する．よって $K \supset F(G)$ となり，$K = F(G)$ が成り立つ．

（2） G を $\mathrm{Aut}(L)$ の有限部分群とし，$K=F(G)$，$n=\sharp G$ とおく．(1) の証明の前半の議論を，$\mathrm{Aut}(L/K)$ をこの有限群 G でおき換え，繰り返す．これにより，任意の $\theta\in L$ は $K=F(G)$ 上代数的かつ分離的で，しかも $[K(\theta):K]=\deg\mathrm{Irr}(\theta,K,x)\leqq\sharp G=n$ なることがわかる．したがって，$[K(\theta):K]$ が最大値をとる $\theta\in L$ が存在する．ところが L/K は分離代数的であり，定理 4.9 より任意の有限次分離拡大は単拡大となるから，θ のとり方より，

$$[L:K]=[K(\theta):K]\leqq n$$

が成り立つ．そうすると，$L=K(\theta)$ となり，L/K は有限次分離拡大となる．よって

$$[L:K]=[L:K]_s\geqq\sharp\{\mathrm{Aut}(L/K)\}\geqq\sharp G=n$$

とが成り立つ．したがって，

$$[L:K]=[L:K]_s=\sharp\{\mathrm{Aut}(L/K)\}=\sharp \mathrm{G}$$

となるから，任意の $\sigma:L\longrightarrow\bar{K}$ なる K-同型は G の元となる．とくに，$\sigma(L)=L$ が成り立つから，L/K は正規になる．したがって，L/K はガロア拡大となり，そのガロア群 $\mathrm{Gal}(L/K)$ は，G と一致する．これで定理が証明された． （証明終）

5. 2 ガロアの基本定理 定理 5.1 を使うと，有限次ガロア拡大における中間体を調べることが，対応するガロア群の部分群を調べることに帰着する．これより，次の定理が得られる．

定理 5. 2 （ガロアの基本定理） L/K を有限次ガロア拡大とし，そのガロア群を $G=\mathrm{Gal}(L/K)$ とする．また，L/K の中間体の全体を $\mathscr{M}$，G の部分群全体を $\mathscr{H}$ で表す．このとき，

（1） M を L/K の中間体とすると，L/M もガロア拡大となり，そのガロア群 $\mathrm{Gal}(L/M)$ は G の部分群となる．そこで，$\varphi:\mathscr{M}\longrightarrow\mathscr{H}$ なる写像を，

$$\varphi(M)=\mathrm{Gal}(L/M)$$

により定める．このとき，φ は全単射で，φ の逆写像は

$$\psi:\quad \mathscr{H}\ni H\longmapsto F(H)\in\mathscr{M}$$

で与えられる．ここで $F(H)=\{a\in L\mid a^\sigma=a\ (\forall\sigma\in H)\}$ は H による不変体である．さらに $\mathscr{M}\ni M$ と $\mathscr{H}\ni H$ がこのようにして対応するとき，

$$[L:M]=\sharp H$$

なる等式が成り立つ．

（2） L/K の中間体 M が K のガロア拡大となるためには，$\varphi(M)=\mathrm{Gal}(L/M)$ が G の正規部分群となることが必要かつ十分である．またこのとき，$G=\mathrm{Gal}(L/K)$ の作用の M への制限により，

$$\mathrm{Gal}(L/K)/\mathrm{Gal}(L/M)\cong\mathrm{Gal}(M/K)$$

なる群の同型が得られる．

[証明] （1） L/K の中間体 M をとると，L/M がガロア拡大で，そのガロア群 $\mathrm{Gal}(L/M)$ が $G=\mathrm{Gal}(L/K)$ の部分群となることは，5.1 でみた．したがって，

$$\varphi:\quad \mathscr{M}\ni M\longmapsto \mathrm{Gal}(L/M)\in\mathscr{H}$$

が定義できる．

$M\in\mathscr{M}$ とすると，L/M はガロア拡大だから，定理 5.1，（1）により，

$$(\sharp)\qquad F(\mathrm{Gal}(L/M))=M$$

が成り立つ．また $H\in\mathscr{H}$ とすると，H は $\mathrm{Aut}(L)$ の有限部分群だから，定理 5.1，（2）より，

$$(\flat)\qquad \mathrm{Gal}(L/F(H))=H,\qquad [L:F(H)]=\sharp H$$

が成り立つ．$H\subset\mathrm{Gal}(L/K)$ だから $F(H)\supset K$ となり，$F(H)\in\mathscr{M}$ が成り立つ．よって

$$\psi:\quad \mathscr{H}\ni H\longmapsto F(H)\in\mathscr{M}$$

が定義できる．ところが，($\sharp$) と ($\flat$) より，φ と ψ は互いに逆写像となることがわかるから，$\varphi:\mathscr{M}\longrightarrow\mathscr{H}$ は全単射である．

（2） L/K が分離的だから，M/K も分離的となり，正規性のみが問題となる．$M\in\mathscr{M}$，$\sigma\in\mathrm{Gal}(L/K)$ のとき，$\sigma(M)=\{\sigma(a)\mid a\in M\}$ である．したがって，$\tau\in\mathrm{Gal}(L/K)$ のとき，

$$\begin{aligned}\tau\in\mathrm{Gal}(L/\sigma(M))\ &\Longleftrightarrow\ \tau\{\sigma(a)\}=\sigma(a)\ \ (\forall a\in M)\\ &\Longleftrightarrow\ (\sigma^{-1}\tau\sigma)(a)=a\ \ (\forall a\in M)\\ &\Longleftrightarrow\ \sigma^{-1}\tau\sigma\in\mathrm{Gal}(L/M)\end{aligned}$$

である．つまり $\varphi(\sigma(M))=\sigma\varphi(M)\sigma^{-1}$ が成り立つ．

さて，L/K は正規拡大だから，L の代数的閉包を $\bar{K}$ とすると，制限写像

$$\tilde{r}:\quad \mathrm{Aut}(\bar{K}/K)\ni\tilde{\sigma}\longmapsto\tilde{\sigma}|_L\in\mathrm{Gal}(L/K)$$

が定義され，しかも定理 2.8,（2）より全射となる．したがって，φ は単射だから，

$$M/K \text{ 正規拡大} \iff \varphi(\sigma(M)) = \varphi(M) \ (\forall \sigma \in \mathrm{Gal}(L/K))$$

が成り立つ．$\varphi(\sigma(M)) = \sigma\varphi(M)\sigma^{-1}$ であるから，これは，$\varphi(M)$ が $G = \mathrm{Gal}(L/K)$ の正規部分群であることと同値である．

M/K が正規だとする．このとき，M への制限写像

$$r: \quad \mathrm{Aut}(L/K) \ni \sigma \longmapsto \sigma|_M \in \mathrm{Gal}(M/K)$$

が定義される．ここで L/K は正規だから，系 3.3 より，r は全射である．ところが，この写像の核は $\mathrm{Gal}(L/M)$ であるから，群の同型 $\mathrm{Gal}(L/K)/\mathrm{Gal}(L/M) \xrightarrow{\sim} \mathrm{Gal}(M/K)$ が成り立つ． （証明終）

命題 5.3 L/K を有限次ガロア拡大，M_1, M_2 を L/K の中間体，H_1, H_2 を対応するガロア群 $\mathrm{Gal}(L/K)$ の部分群とする．このとき，

（1） $M_1 \supseteqq M_2 \iff H_1 \subseteqq H_2$

（2） 合成体 $M_1 \cdot M_2$ には $H_1 \cap H_2$ が，交り $M_1 \cap M_2$ には H_1 と H_2 で生成される部分群 $\langle H_1, H_2 \rangle$ が対応する．とくに，M_1, M_2 が K 上ガロア拡大なら，$M_1 \cdot M_2$ と $M_1 \cap M_2$ も K のガロア拡大となる．

［証明］（1） は 5.1 で注意した．

（2） $\sigma = \mathrm{id}$ on $M_1 \cdot M_2 \iff \sigma = \mathrm{id}$ on M_1 かつ $\sigma = \mathrm{id}$ on M_2

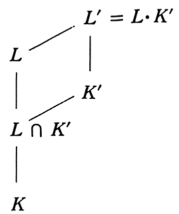
だから，$M_1 \cdot M_2$ には $H_1 \cap H_2$ が対応する．また $M_1 \cap M_2 \subset M_1$, M_2 だから，$M_1 \cap M_2$ に対応する部分群を H とすると，(1) より $H \supset H_1, H_2$ である． よって $H \supset \langle H_1, H_2 \rangle$ である． そこで $\langle H_1, H_2 \rangle$ に対応する L/K の部分体を M' とする． このとき $\langle H_1, H_2 \rangle \supset H_1, H_2$ だから，$M' \subset M_1, M_2$ となり，$M' \subset M_1 \cap M_2$ となる．したがって $\langle H_1, H_2 \rangle \supset H$ である．よって $H = \langle H_1, H_2 \rangle$, $M' = M_1 \cap M_2$ が成り立つ．

$H_1, H_2 \lhd \mathrm{Gal}(L/K)$ なら，$H_1 \cap H_2$, $\langle H_1, H_2 \rangle \lhd \mathrm{Gal}(L/K)$ となるから，後半は明らかである． （証明終）

命題 5.4 L/K を有限次ガロア拡大，K'/K を任意の拡大，$L' = L \cdot K'$ を合成体とする．このとき L'/K' も有限次ガロア拡大で，そのガロア群は $L/L \cap K'$ のガロア群と同型となる．

（注） この命題では，L と K' は共にある体に入っていて，その部分体として合成体が

作れるものと仮定する．この場合，L と K' が入っている体は，余り問題にならないから，単に「$L \cdot K'$ を合成体とする」と表現した．系 4.6 や次の命題 5.5 でも，同様の表現方法を使っている．



［証明］ L/K が有限次，正規，かつ分離的なら，$L' = K'(L)$ も K' 上有限次，分離的なことは明らかである．$\sigma : L' \longrightarrow \bar{L}'$ を L' の代数的閉包 $\bar{L}'$ の中への K'–同型とする．$K' \supset K$ だから，σ は K–同型である．ところが L/K は正規だから，$\sigma(L) = L$ となり，$\sigma(L') = K'(\sigma(L)) = K'(L) = L'$ が成り立つ．よって L'/K' は正規である．よって L'/K' も有限次ガロア拡大である．

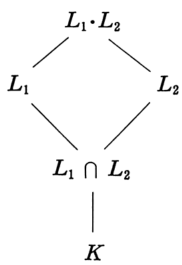
$\sigma \in \mathrm{Gal}(L'/K')$ を L に制限すると，$L/L \cap K'$ は正規で，σ は $L \cap K'$ の各元を動かさないから，

$$f: \quad \mathrm{Gal}(L'/K') \ni \sigma \quad \longmapsto \quad \sigma|_L \in \mathrm{Gal}(L/L \cap K')$$

なる準同型ができる．σ がこの写像の核に入れば，σ は L 上自明だから，$L' = K' \cdot L$ 上で id となる．よって f は単射である．

$H = \{\sigma|_L \mid \sigma \in \mathrm{Gal}(L'/K')\}$ とおき，H に対応する L/K の部分体を考える．$\sigma|_L$ で不変な L の元とは，σ で不変な L の元のことだから，H には $L \cap K'$ が対応する．よって定理 5.1，(1)，(2) より，$f : \mathrm{Gal}(L'/K') \longrightarrow \mathrm{Gal}(L/L \cap K')$ は全射である．

（証明終）



命題 5.5　L_1, L_2 を K の有限次ガロア拡大とする．このとき，$L_1 \cdot L_2$，$L_1 \cap L_2$ は共にガロア拡大で，これらのガロア群の間には，完全列

$$\begin{aligned} 1 &\longrightarrow \mathrm{Gal}(L_1 \cdot L_2/L_1 \cap L_2) \\ &\longrightarrow \mathrm{Gal}(L_1 \cdot L_2/K) \\ &\longrightarrow \mathrm{Gal}(L_1 \cap L_2/K) \longrightarrow 1 \end{aligned}$$

と，同型

$$\mathrm{Gal}(L_1 \cdot L_2/L_1 \cap L_2) \simeq \mathrm{Gal}(L_1/L_1 \cap L_2) \times \mathrm{Gal}(L_2/L_1 \cap L_2)$$

が成り立つ．とくに

$$L_1 \cap L_2 = K \iff [L_1 \cdot L_2 : K] = [L_1 : K][L_2 : K]$$
$$\iff \mathrm{Gal}(L_1 \cdot L_2/K) = \mathrm{Gal}(L_1/K) \times \mathrm{Gal}(L_2/K)$$

が成り立つ．

［証明］ L_1, L_2は共にK上有限次，正規，分離的だから，$L_1 \cdot L_2$も$L_1 \cap L_2$もK上同様である．

$L_1 \cap L_2$がK上正規だから，系3.3より，制限写像

$$\mathrm{Gal}(L_1 \cdot L_2/K) \ni \sigma \longmapsto \sigma|_{L_1 \cap L_2} \in \mathrm{Gal}(L_1 \cap L_2/K)$$

は全射な準同型となる．しかも，この写像の核は$\mathrm{Gal}(L_1 \cdot L_2/L_1 \cap L_2)$だから，命題の完全列が得られる．

命題5.3より，$\mathrm{Gal}(L_1 \cdot L_2/L_1 \cap L_2)$は$\mathrm{Gal}(L_1 \cdot L_2/L_1)$と$\mathrm{Gal}(L_1 \cdot L_2/L_2)$で生成される．しかも$\mathrm{Gal}(L_1 \cdot L_2/L_1) \cap \mathrm{Gal}(L_1 \cdot L_2/L_2)$に対応する$\mathrm{Gal}(L_1 \cdot L_2/L_1 \cap L_2)$の部分体は$L_1 \cdot L_2$だから，$\mathrm{Gal}(L_1 \cdot L_2/L_1) \cap \mathrm{Gal}(L_1 \cdot L_2/L_2) = \{1\}$である．ところが$L_1/K$，$L_2/K$は正規だから，$\mathrm{Gal}(L_1 \cdot L_2/L_1), \mathrm{Gal}(L_1 \cdot L_2/L_2) \lhd \mathrm{Gal}(L_1 \cdot L_2/L_1 \cap L_2)$となり，

$$\mathrm{Gal}(L_1 \cdot L_2/L_1 \cap L_2) \simeq \mathrm{Gal}(L_1 \cdot L_2/L_1) \times \mathrm{Gal}(L_1 \cdot L_2/L_2)$$

と直積になる（第II章，定理5.2参照）．ここで命題5.4より，

$$\mathrm{Gal}(L_1 \cdot L_2/L_1) \simeq \mathrm{Gal}(L_2/L_1 \cap L_2), \qquad \mathrm{Gal}(L_1 \cdot L_2/L_2) \simeq \mathrm{Gal}(L_1/L_1 \cap L_2)$$

であるから，命題の前半が証明された．命題の後半は，いずれの条件も$[L_1 \cap L_2 : K] = 1$を意味することより明らかである． （証明終）

5.3 方程式のガロア群

まず次のことに注意しておく．

命題 5.6 L/Kが有限次ガロア拡大であるための必要十分条件は，Lがある分離的既約多項式$f(x) \in K[x]$の分解体となることである．

［証明］ L/Kが有限次ガロア拡大なら，有限次分離拡大となり，定理4.9より，LはKの単拡大となる．$L = K(\theta)$とし，$f(x) = \mathrm{Irr}(\theta, K, x)$とおくと，$f(x)$は分離的既約方程式である．ところが$L/K$は正規だから，$L$は$f(x)$のすべての根を含み，$f(x)$の分解体となる．

逆にL/Kが分離的多項式$f(x) \in K[x]$の分解体なら，命題4.5より，L/Kは有限次分離拡大である．また定理3.5より，L/Kは正規拡大にもなる．よってL/Kは有限

次ガロア拡大である. (証明終)

この命題により，有限次ガロア拡大 L/K を調べることは，K 上の分離的既約多項式 $f(x)\in K[x]$ の分解体を調べることと同値である.

一般に，$f(x)\in K[x]$ を分離的多項式とするとき，その分解体 L の K 上のガロア群

$$G=\mathrm{Gal}(L/K)$$

を，**方程式 $f(x)=0$ のガロア群** とよぶ. そこでガロア群 G が 巡回群，アーベル群，… となるのに応じて，$f(x)\in K[x]$ を **巡回方程式**，**アーベル方程式**，… とよぶ.

$f(x)=0$ の L での根を $\theta_1,\theta_2,\cdots,\theta_n$ とする. このとき $\sigma\in G$ は，$\{\theta_1,\theta_2,\cdots,\theta_n\}$ の置換をひきおこす. これにより，G の $\{\theta_1,\theta_2,\cdots,\theta_n\}$ の置換群としての表現（第Ⅱ章，§3参照）

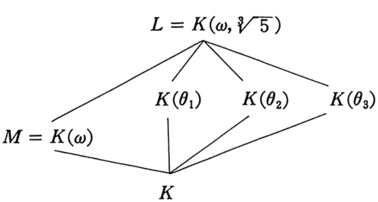
$$\rho:\quad G\longrightarrow S(\{\theta_1,\theta_2,\cdots,\theta_n\})\simeq S_n$$

ができる. しかも $\sigma\in\mathrm{Gal}(L/K)$ は，$L=K(\theta_1,\theta_2,\cdots,\theta_n)$ だから，各 θ_i をどの根に移すかを決めれば定まる. したがって，この表現 ρ は単射となり，これにより，G は対称群 S_n の部分群とみなせる.

例 5.7 $K=\boldsymbol{Q}$, $f(x)=x^3-5$ とする. 例1.8より，$f(x)$ の K の分解体は $L=K(\omega,\sqrt[3]{5})$ $(\omega=(-1+\sqrt{-3})/2)$ であり，$f(x)$ の根は，

$$\theta_1=\sqrt[3]{5},\quad \theta_2=\omega\sqrt[3]{5},\quad \theta_3=\omega^2\sqrt[3]{5}$$

の3つである. $K=\boldsymbol{Q}$ は標数0の体だから，$f(x)$ は分離的多項式である.



5は素数で，$\omega\notin\boldsymbol{R}$ だから，

$$[L:K]=[K(\sqrt[3]{5})(\omega):K(\sqrt[3]{5})][K(\sqrt[3]{5}):K]=2\cdot3=6$$

である. また $M=K(\omega)$ は K の2次拡大で，ω の共役元は $\omega^2\in M$ だから，M/K は正

規である．したがって，

$$1 \longrightarrow \mathrm{Gal}(L/M) \longrightarrow \mathrm{Gal}(L/K) \longrightarrow \mathrm{Gal}(M/K) \longrightarrow 1$$

なる完全列があり，$\#\mathrm{Gal}(L/M)=3$, $\#\mathrm{Gal}(M/K)=2$ となる．したがって，$\mathrm{Gal}(L/M) \simeq \boldsymbol{Z}/3\boldsymbol{Z}$, $\mathrm{Gal}(M/K) \simeq \boldsymbol{Z}/2\boldsymbol{Z}$ となるから，$\mathrm{Gal}(L/K) \simeq S_3$ となる．(一般に3次方程式のガロア群は，S_3 の部分群で位数が3の倍数だから，S_3 か $\boldsymbol{Z}/3\boldsymbol{Z}$ と同型となる．)

この場合，G を具体的に計算すると，$L=K(\omega,\theta_1)$ だから，

$$G=\langle\sigma,\tau\rangle$$
$$\sigma(\omega)=\omega^2, \qquad \sigma(\theta_1)=\theta_1$$
$$\tau(\omega)=\omega, \qquad \tau(\theta_1)=\omega\theta_1$$

となる．したがって

$$(\sigma^{-1}\circ\tau\circ\sigma)(\omega)=\omega, \qquad (\sigma^{-1}\circ\tau\circ\sigma)(\theta_1)=\omega^2\theta_1$$

だから，G の基本関係（第II章，§9参照）は

$$\sigma^2=\mathrm{id}, \qquad \tau^3=\mathrm{id}, \qquad \sigma^{-1}\circ\tau\circ\sigma=\tau^2$$

となり，$G \simeq S_3$ となることが確かめられる．

例 5.8 体 k 上の n 変数有理関数体を $L=k(x_1,x_2,\cdots,x_n)$ とし，対称群 S_n を $f(x_1,x_2,\cdots,x_n)\in L$ に，

$$\sigma(f)(x_1,x_2,\cdots,x_n)=f(x_{\sigma(1)},x_{\sigma(2)},\cdots,x_{\sigma(n)})$$

で作用させる．これにより，$\sigma\in S_n$ が

$$L\ni f \longmapsto \sigma(f)\in L$$

として L に作用し，$S_n\subset \mathrm{Aut}(L)$ と思える．

多項式環 $L[x]$ において，

$$\begin{aligned} S(x) &= (x-x_1)(x-x_2)\cdots(x-x_n) \\ &= x^n - s_1x^{n-1}+\cdots+(-1)^{n-1}s_{n-1}x+(-1)^n s_n \end{aligned}$$

と展開し，その係数

$$s_i=s_i(x_1,x_2,\cdots,x_n)\in L \qquad (1\leqq i\leqq n)$$

を，$x_1,x_2,\cdots,x_n$ の **基本対称式** とよぶ．これは明らかに，任意の $\sigma\in S_n$ の上の作用で不変である．

一般に，$L=k(x_1,x_2,\cdots,x_n)$ の元で，任意の $\sigma\in S_n$ の作用で不変なものを $x_1,x_2,\cdots,x_n$ の **対称式** とよぶ．$x_1,x_2,\cdots,x_n$ の対称式全体を K とおくと，定理5.1,(2)より，L/K

は $n!$ 次のガロア拡大で，$\mathrm{Gal}(L/K) \simeq S_n$ となる．明らかに，

$$L \supset K \supset k(s_1, s_2, \cdots, s_n)$$

であるが，$L = k(x_1, x_2, \cdots, x_n)$ は $K^* = k(s_1, s_2, \cdots, s_n)$ 上 $S(x) \in K^*[x]$ の根 $x_1, x_2, \cdots, x_n$ により生成される．つまり，L/K^* は n 次方程式 $S(x)$ の分解体となる．したがって，L/K^* のガロア群は対称群 S_n の部分群となり(209ページ参照)，

$$[L : K^*] \leqq \# S_n$$

が成り立つ．ところが，

$$L \supset K \supset K^*, \qquad [L : K] = \# \mathrm{Gal}(L/K) = \# S_n$$

であるから，$K = K^*$ となる．したがって，

（1） $x_1, x_2, \cdots, x_n$ の任意の対称式は，基本対称式 $s_1, s_2, \cdots, s_n$ の有理式として書け，

（2） $k(x_1, x_2, \cdots, x_n)/k(s_1, s_2, \cdots, s_n)$ は有限次ガロア拡大で，そのガロア群は対称群 S_n と同型になる．

（注） この例の（1）は，第 I 章末の問題 3,（1）の漸化式を使っても証明できる．その場合，$x_1, x_2, \cdots, x_n$ の多項式で対称式となるものは，基本対称式 $s_1, s_2, \cdots, s_n$ の多項式で書けることが証明できる．

5.4 代数学の基本定理 次の定理はガウスにより証明され，現在では何通りもの証明があるが，ここでは，ガロアの理論を応用した証明を与える．

定理 5.9 （代数学の基本定理） 複素数体 $\boldsymbol{C}$ は代数的閉体である．

［証明］ まず次の2つのことを証明する：

（1） 実数体 $\boldsymbol{R}$ の奇数次の拡大体は $\boldsymbol{R}$ に限る．

（2） $\boldsymbol{C}$ の2次拡大体は存在しない．

（1）を示すため，$L_1 = \boldsymbol{R}(\theta_1)$ を $2m+1$ 次（$m > 0$）の $\boldsymbol{R}$ の代数拡大とする．このとき，θ_1 の最小多項式は，

$$f_1(x) = x^{2m+1} + a_{2m} x^{2m} + \cdots + a_1 x + a_0 \in \boldsymbol{R}[x]$$

の形であり，

$$\lim_{x \to +\infty} f_1(x) = +\infty, \qquad \lim_{x \to -\infty} f_1(x) = -\infty$$

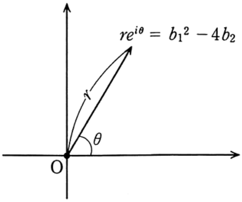
を満たす．したがって，中間値の定理より，$x_0 \in \boldsymbol{R}$ で $f(x_0) = 0$ となるものが存在し，$f_1(x)$ は $x - x_0 \in \boldsymbol{R}[x]$ で割り切れる．$\deg f(x) = 2m+1 > 1$ だから，これは $f_1(x)$

の既約性に矛盾する．

(2) については，$L_2 = \boldsymbol{C}(\theta_2)$ を $\boldsymbol{C}$ の 2 次拡大とし，その最小多項式を

$$f_2(x) = x^2 + b_1 x + b_2 \in \boldsymbol{C}[x]$$

とする．このとき $f_2(x) = 0$ の 2 根は，$(-b_1 \pm \sqrt{b_1{}^2 - 4b_2})/2$ である．ところが，



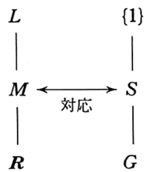
$$re^{i\theta} = b_1{}^2 - 4b_2 \qquad (r \geqq 0,\ 2\pi > \theta \geqq 0)$$

と極表示をすると，

$$\sqrt{b_1{}^2 - 4b_2} = \sqrt{r}\, e^{i\theta/2} \in \boldsymbol{C}$$

である．したがって，$f_2(x)$ は根 $(-b_1 \pm \sqrt{r}\, e^{i\theta/2})/2 \in \boldsymbol{C}$ を持つから，$\boldsymbol{C}[x]$ において既約ではない．

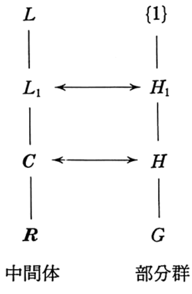
以上の準備のもとで定理を証明する．



α を $\boldsymbol{C}$ 上代数的な元とし，$\boldsymbol{R}$ の有限次ガロア拡大 L で，$\boldsymbol{C}(\alpha)$ を含むものをとる．$G = \mathrm{Gal}(L/\boldsymbol{R})$ を $L/\boldsymbol{R}$ のガロア群とし，その 2–シロー部分群を S，S に対応する $L/\boldsymbol{R}$ の部分体を M とする．このとき，

$$[M : \boldsymbol{R}] = \sharp G / \sharp S$$

は奇数となる．よって (1) より，$M = \boldsymbol{R}$ となり，$G = S$ は 2–群となる．



G の部分群で $\boldsymbol{C}$ に対応するものを H とする．$L = \boldsymbol{C}$ なら $\alpha \in \boldsymbol{C}$ となるから，$L \supsetneqq \boldsymbol{C}$ とし，したがって $H \neq \{1\}$ とする．$H \subset G$ も 2–群だから，第 II 章，定理 8.22 よりべき零群である．よって H の極大部分群を H_1 とすると，H_1 は H で正規で，$H/H_1 \simeq \boldsymbol{Z}/2\boldsymbol{Z}$ となる．そこで H_1 に対応する L の部分体を L_1 とすると，

$$L \supset L_1 \supset \boldsymbol{C}, \qquad [L_1 : \boldsymbol{C}] = \sharp(H/H_1) = 2$$

となる．これは (2) に矛盾する．　　　　（証明終）

§6. 円分体と有限体

6.1 円分体　K を体とするとき，K の元 ζ で $\zeta^m = 1$ $(m \in \boldsymbol{N})$ となる

ものを，**1の m 乗根** とよぶ．m にとくにふれる必要のないときは，単に，**1のべき根** とよぶ．1の m 乗根 ζ で，$1 \leqq d < m$ なる d に対しては $\zeta^d \neq 1$ となるものを **1の原始 m 乗根** とよぶ．

命題 6.1　K を体とし，S を K の乗法群 $K^* = K \setminus \{0\}$ の有限部分群，S の元の個数を m とする．このとき S は巡回群で，その生成元は原始 m 乗根である．

［証明］　d を m の任意の約数とし，

$$\{x \in S \mid x^d = 1\}$$

を考える．これは，体 K での d 次方程式 $x^d = 1$ の根の集合であるから，（第Ⅰ章，問題9.3より）高々 d 個の元から成る．したがって，S は位数 m のアーベル群で，m の任意の約数 d に対し，S の元で位数が d の約数となるものの個数は高々 d 個である．したがって，アーベル群の基本定理（第Ⅱ章，定理6.2）より，S は位数 m の巡回群となる（第Ⅱ章，問題6.4参照）．S の生成元が原始 m 乗根であることは，$S \simeq \boldsymbol{Z}/m\boldsymbol{Z}$ より明らかである．　（証明終）

命題 6.2　Ω を代数的閉体とするとき，次は同値である．

（1）　Ω は1の原始 m 乗根を含む．

（2）　Ω の1の m 乗根の全体は，位数 m の巡回群をなす．

（3）　Ω の標数を p とすると，m は p では割れない．

［証明］（2）$\Longrightarrow$（1）は明らかである．

（1）$\Longrightarrow$（3）．　$p > 0$，$m = pn$ とし，$\zeta \in \Omega$ を原始 m 乗根とする．このとき $(\zeta^n)^p = \zeta^m = 1$ である．ところが，標数 p の体では，写像 $x \longmapsto x^p$ は単射となるから，$\zeta^n = 1$ となる（4.1参照）．これは矛盾である．

（3）$\Longrightarrow$（2）．　Ω の標数 p で m が割り切れないとする．このとき $f(x) = x^m - 1 \in \Omega[x]$ は $f'(x) = mx^{m-1} \neq 0$ を満たし，分離多項式である（4.2参照）．ところが Ω は代数的閉体であるから，$f(x)$ は Ω において1次式の積となり，

$$f(x) = \prod_{1 \leq i \leq m} (x - \zeta_i) \qquad (i \neq j \text{ なら } \zeta_i \neq \zeta_j)$$

の形となる．したがって，$S = \{\zeta \in \Omega \mid \zeta^m = 1\}$ はちょうど m 個の元から成るから，命題6.1により（2）が成り立つ．　（証明終）

K を標数 p の体とし, m を p で割り切れない自然数とする. K の代数的閉包を $\bar{K}$ とすると，命題6.2より，$\bar{K}$ は1の原始 m 乗根を含む. そこで $\bar{K}$ の原始 m 乗根を1つとり，それを ζ_m で表す.

$L = K(\zeta_m)$ とおく. ζ_m は分離的多項式 $f(x) = x^m - 1 \in K[x]$ の根だから，L/K は分離的である. また $\sigma \in \mathrm{Aut}(\bar{K}/K)$ に対し，$\sigma(\zeta_m)$ も $f(x)$ の根で，原始 m 乗根である. したがって，命題6.2の証明より，

$$\sigma(\zeta_m) = (\zeta_m)^i \qquad (1 \leqq i \leqq m,\ (i, m) = 1)$$

と書ける. これは $L = K(\zeta_m)$ に入るから，L/K は正規であり，有限次ガロア拡大となる. そこで L/K のガロア群 $\mathrm{Gal}(L/K)$ を G で表す.

$\sigma \in G$ に対し，i を上のようにとり，環 $\boldsymbol{Z}/m\boldsymbol{Z}$ の単数のなす群への写像

$$h:\quad G \ni \sigma \longmapsto i \pmod{m} \in U(\boldsymbol{Z}/m\boldsymbol{Z})$$

を作る. これは $\sigma(\zeta_m) = (\zeta_m)^i$ なる定義式より，群の準同型写像となることがわかる. また，$\sigma(\zeta_m) = \zeta_m$ なら，σ は $K(\zeta_m)/K$ のガロア群の元として id となるから，h は単射である. したがって，G は $U(\boldsymbol{Z}/m\boldsymbol{Z})$ の部分群と同型となる.

$K = \boldsymbol{Q}$ とする. このとき，$L = \boldsymbol{Q}(\zeta_m)$ を **1の m 等分点の体** という. また $f(x) = x^m - 1$ の一部である

$$\Phi_m(x) = \prod (x - \zeta_m{}^i) \qquad (1 \leqq i \leqq m,\ (i, m) = 1)$$

を，**円分多項式** とよぶ. $\sigma \in \mathrm{Gal}(\boldsymbol{Q}(\zeta_m)/\boldsymbol{Q})$ は，$\zeta_m \longmapsto (\zeta_m)^i$ $(1 \leqq i \leqq m,$ $(i, m) = 1)$ の形の元の置換をひきおこすから，$\Phi_m(x)$ は $\mathrm{Gal}(\boldsymbol{Q}(\zeta_m)/\boldsymbol{Q})$ で動かず，したがって，$\boldsymbol{Q}$-係数の多項式となる.

円分多項式について，

（1）　$\deg \Phi_m(x) = \sharp\, U(\boldsymbol{Z}/m\boldsymbol{Z}) = \varphi(m)$　　（オイラーの関数）

（2）　$x^m - 1 = \prod_{d \mid m} \Phi_d(x)$

が成り立つことは明らかであるが，さらに次の補題が成り立つ.

補題6.3　円分多項式 $\Phi_m(x) \in \boldsymbol{Q}[x]$ は $\boldsymbol{Q}$ 上既約である.

補題が証明できれば，

$$[\boldsymbol{Q}(\zeta_m):\boldsymbol{Q}]=\deg \Phi_m(x)=\# U(\boldsymbol{Z}/m\boldsymbol{Z})$$

となることがわかる．したがって，

$$\# G=[\boldsymbol{Q}(\zeta_m):\boldsymbol{Q}]=\# U(\boldsymbol{Z}/m\boldsymbol{Z})$$

となるから，$h: G \longrightarrow U(\boldsymbol{Z}/m\boldsymbol{Z})$ なる準同型は全射になる．したがって，次の定理が成り立つ．

定理 6.4　K の標数が m と素なら，K 上 1 の原始 m 乗根 ζ_m の生成する体を L とおくと，L/K は有限次ガロア拡大で，そのガロア群 G は $U(\boldsymbol{Z}/m\boldsymbol{Z})$ の部分群と同型となる．とくに $K=\boldsymbol{Q}$ の場合は，$\boldsymbol{Q}(\zeta_m)/\boldsymbol{Q}$ は有限次ガロア拡大で，そのガロア群は $U(\boldsymbol{Z}/m\boldsymbol{Z})$ と同型になる．

[補題 6.3 の証明]　まず $\Phi_m(x)\in\boldsymbol{Z}[x]$ なることを，mに関する帰納法で示す．

帰納法の仮定より，$f(x)=\prod \Phi_d(x)$ $(1\leqq d<m,\ d\mid m)$ は $\boldsymbol{Z}[x]$ の元である．しかも，最高次の係数が 1 だから，原始多項式である．ところが

$$x^m-1=\Phi_m(x)f(x)$$

であるから，ガウスの補題（第Ⅲ章，補題 4.10）より，$\Phi_m(x)\in\boldsymbol{Q}[x]$ も $\boldsymbol{Z}[x]$ に属す．

ζを 1 の原始 m 乗根とし，$g(x)$ をζを根とする 既約かつ原始的な $\boldsymbol{Z}[x]$ の多項式とする．このとき，$g(x)$ は $\Phi_m(x)$ を割り切るから，

$$\Phi_m(x)=g(x)h(x)$$

となる $h(x)\in\boldsymbol{Z}[x]$ が存在する．

pを m と素な任意の素数とする．このとき，ζ^p もまた 1 の原始 m 乗根となるから，$g(\zeta^p)=0$ または $h(\zeta^p)=0$ となる．もし $h(\zeta^p)=0$ なら，$h(x^p)$ はζを根にもつから，

$$h(x^p)=g(x)i(x)$$

となる $i(x)\in\boldsymbol{Z}[x]$ が存在する．そこで $\bmod p$ をとることにより，$\boldsymbol{Z}[x]\longrightarrow(\boldsymbol{Z}/p\boldsymbol{Z})[x]$ なる写像を作り，$j(x)\in\boldsymbol{Z}[x]$ の像を $\bar{j}(x)$ で表す．この写像は環の準同型だから，

$$\bar{g}(x)\bar{i}(x)=\bar{h}(x^p)=\{\bar{h}(x)\}^p$$

が成り立つ．したがって，$\bar{g}(x)$ と $\bar{h}(x)$ は共通根をもつ．ところが

$$\bar{g}(x)\bar{h}(x)=\bar{\Phi}_m(x)\mid(x^m-1)$$

は $(\boldsymbol{Z}/p\boldsymbol{Z})[x]$ の分離的多項式であるから，これは矛盾である．したがって $g(\zeta^p)=0$ となる．

以上より，ζ が1の原始 m 乗根で，p が m と素な素数なら，ζ^p も $g(x)$ の根となることがわかった．$1\leqq i<m$，$(i,m)=1$ とし，$i=p_1p_2\cdots p_t$ を素因数分解とする．このとき，帰納法により，$g(x)$ は ζ，ζ^{p_1}，$(\zeta^{p_1})^{p_2}$，…，$(\zeta^{p_1p_2\cdots p_{t-1}})^{p_t}=\zeta^i$ を根とする．よって $g(x)$ は $\Phi_m(x)=\prod_i(x-\zeta^i)$ で割り切れる．よって，$g(x)=\Phi_m(x)$ となるから，$\Phi_m(x)$ は既約である． (証明終)

(注)* 一般に $\boldsymbol{Q}(\zeta_m)/\boldsymbol{Q}$ の中間体を **円分体** とよぶ．定理6.4より円分体は $\boldsymbol{Q}$ の有限次アーベル拡大となるが，逆に，$\boldsymbol{Q}$ の有限次アーベル拡大は円分体となることがわかっている（クロネッカーの定理）.

$\Phi_m(x)\in\boldsymbol{Z}[x]$ を円分多項式，p を m と素な素数とし，

$$\bar{\Phi}_m(x)=\Phi_m(x)\pmod p\in(\boldsymbol{Z}/p\boldsymbol{Z})[x]$$

とおく．他方，有限群 $U(\boldsymbol{Z}/m\boldsymbol{Z})$ の中での $p\ (\mathrm{mod}\ m)$ の位数を g とし，$\#U(\boldsymbol{Z}/m\boldsymbol{Z})=gt$ とおく．このとき

（1） $\bar{\Phi}_m(x)$ は相異なる t 個の g 次既約多項式の積に因数分解され，

（2） 有限体 $\boldsymbol{F}_p=\boldsymbol{Z}/p\boldsymbol{Z}$ 上，$\bar{\zeta}_m=\zeta_m\pmod p$ は g 次の拡大体を生成する，

ことが証明できる．これは，円分体における分解法則とよばれ，類体論の原型を与える．

6.2 有限体 K を有限個の元から成る体とし，その元の個数を q とする．K の素体を K_0 とすると，K_0 も有限個の元より成るから，例1.1より，$\#K_0=p$ は素数で，$K_0\simeq\boldsymbol{Z}/p\boldsymbol{Z}$ となる．K_0 の代数的構造は p により一意的に定まるから，$K_0=\boldsymbol{F}_p$ とおく．

拡大次数 $[K:\boldsymbol{F}_p]$ を n とおく．このとき，K は $\boldsymbol{F}_p$ 上の n 次元のベクトル空間となるから，加法群として $\boldsymbol{F}_p$ の n 個の直和 $(\boldsymbol{F}_p)^n$ と同型になる．したがって，$q=\#(\boldsymbol{F}_p)^n=p^n$ となる．

$\boldsymbol{F}_p$ の K を含む代数的閉包を $\bar{\boldsymbol{F}}_p$ とおく．K の乗法群 $K^*=K\setminus\{0\}$ は $q-1$ 個の元から成る群であるから，命題6.1より巡回群となる．また $K^*\subset\{a\in\bar{\boldsymbol{F}}_p\mid a^{q-1}=1\}$ であるが，$a^{q-1}=1$ は a について $q-1$ 次の方程式だから，高々 $q-1$ 個しか解をもたない．よって

$$K^* = \{a \in \bar{\boldsymbol{F}}_p \mid a^{q-1} = 1\}$$

となる．したがって，

$$K = \{a \in \bar{\boldsymbol{F}}_p \mid a^q = a\}$$

となる．とくに，$\bar{\boldsymbol{F}}_p$ の部分体で q 個の元から成るものは，高々 1 つしか存在しない．

逆に q を素数のべき p^n であるものとし，素体 $\boldsymbol{F}_p = \boldsymbol{Z}/p\boldsymbol{Z}$ の代数的閉包を $\bar{\boldsymbol{F}}_p$ とし，

$$K = \{a \in \bar{\boldsymbol{F}}_p \mid a^q = a\}$$

とおく．$\bar{\boldsymbol{F}}_p$ において q 乗フロベニウス写像（4.1 参照）$a \longmapsto a^q$ は体の自己同型を与えるから，K は $\bar{\boldsymbol{F}}_p$ の部分体である．また

$$f(x) = x^q - x \in \boldsymbol{F}_p[x]$$

は，$f'(x) = qx^{q-1} - 1 = -1$ だから重根をもたぬ．したがって，$f(x)$ の根の全体である K は，q 個の元から成り，$K/\boldsymbol{F}_p$ は分離拡大となる．K は $f(x)$ の分解体をなすから，$K/\boldsymbol{F}_p$ は n 次のガロア拡大となる．

以上をまとめると次の定理を得る．

定理 6.5 （1） 有限体の元の個数 q は素数 p のべきである．

（2） 任意の素数のべき $q = p^n$ に対し，q 個の元から成る有限体が唯一つ存在する．これを $\boldsymbol{F}_q$ と表す．

（3） $\boldsymbol{F}_q$ は素体 $\boldsymbol{F}_p$ 上分離的で，多項式 $x^q - x$ の分解体をなす．また $\boldsymbol{F}_q$ の乗法群は，位数 $q-1$ の巡回群をなす．

有限体の間の代数拡大については，次の定理が成り立つ．

定理 6.6 $\boldsymbol{F}_q$ を q 個の元から成る有限体とする．このとき，$\boldsymbol{F}_{q^m}$ は $\boldsymbol{F}_q$ の m 次拡大で，$\boldsymbol{F}_q$ の m 次拡大は $\boldsymbol{F}_{q^m}$ に限る．また $\boldsymbol{F}_{q^m}/\boldsymbol{F}_q$ は m 次巡回拡大で，そのガロア群は，

$$\sigma: \quad \boldsymbol{F}_{q^m} \ni a \longmapsto a^q \in \boldsymbol{F}_{q^m}$$

により生成される．

[証明] $q=p^n$ とすると，$\boldsymbol{F}_q$ の m 次拡大は $\boldsymbol{F}_p$ の mn 次の拡大であるから，前半は定理6.5より明らかである．

σ が体 $\boldsymbol{F}_{q^m}$ の自己同型をなすことは，4.1で確かめた．しかも，

$$\sigma(a)=a \iff a^q=a \iff a\in\boldsymbol{F}_q$$

であるから，$\sigma\in\mathrm{Gal}(\boldsymbol{F}_{q^m}/\boldsymbol{F}_q)$ である．さらに，$1\leqq i<m$ なら，

$$\{a\in\boldsymbol{F}_{q^m}\mid\sigma^i(a)=a\}=\boldsymbol{F}_{q^m}\cap\boldsymbol{F}_{q^i}\subsetneqq\boldsymbol{F}_{q^m}$$

となるから，$\sigma\in\mathrm{Gal}(\boldsymbol{F}_{q^m}/\boldsymbol{F}_q)$ の位数はちょうど m である．ところが $\sharp\mathrm{Gal}(\boldsymbol{F}_{q^m}/\boldsymbol{F}_q)$ $=[\boldsymbol{F}_{q^m}:\boldsymbol{F}_q]=m$ だから，$\mathrm{Gal}(\boldsymbol{F}_{q^m}/\boldsymbol{F}_q)$ は σ で生成される巡回群となる．(証明終)

問題6.7 $\zeta=\exp(2\pi i/7)$ とおくとき，拡大 $\boldsymbol{Q}(\zeta)/\boldsymbol{Q}$ の中間体をすべて求めよ．

問題6.8 $\boldsymbol{F}_q$ を q 個の元から成る有限体とするとき，

$$K=\bigcup_{1\leq n<\infty}\boldsymbol{F}_{p^n}$$

が $\boldsymbol{F}_p$ の代数的閉包を与えることを示せ．

§7. トレースとノルム

7.1 トレースとノルム L/K を m 次分離拡大とし，L を含む K の代数的閉包を $\bar{K}$ とする．$\{\sigma_1,\sigma_2,\cdots,\sigma_m\}$ を $\sigma:L\longrightarrow\bar{K}$ なる K-同型の全体とし，N を L を含む K の最小のガロア拡大とする（例4.8参照）．

G を N/K のガロア群とするとき，任意の $\tau\in G$ に対し $\{\tau\sigma_1,\tau\sigma_2,\cdots,\tau\sigma_m\}$ も K-同型 $L\longrightarrow\bar{K}$ を与え，全体として $\{\sigma_1,\sigma_2,\cdots,\sigma_m\}$ と一致する．したがって，$\alpha\in L$ に対し，$N[x]$ の多項式

$$F(\alpha;x)=(x-\sigma_1(\alpha))(x-\sigma_2(\alpha))\cdots(x-\sigma_m(\alpha))$$

は $K[x]$ に属する．これを $\alpha\in L$ の K 上の**特性多項式**とよぶ．$F(\alpha;x)$ の根は，α の K 上の共役のみから成るから，

$$F(\alpha;x)=\{\mathrm{Irr}(\alpha,K,x)\}^d,\qquad d=[L:K(\alpha)]$$

となる．

$F(\alpha;x)$ の係数は，$\sigma_1(\alpha),\sigma_2(\alpha),\cdots,\sigma_m(\alpha)$ の基本対称式に符号 $\pm$ をつけた

ものである．そこで

$$Tr_{L/K}(\alpha) = \sigma_1(\alpha) + \sigma_2(\alpha) + \cdots + \sigma_m(\alpha)$$
$$N_{L/K}(\alpha) = \sigma_1(\alpha)\cdot\sigma_2(\alpha)\cdot\cdots\cdot\sigma_m(\alpha)$$

とおき，各々 α の**トレース**および**ノルム**とよぶ（K-加群 L/K に対する第Ⅳ章，例 7.7 の $\mathrm{tr}\,\rho$ 参照）．$Tr_{L/K}(\alpha)$ と $N_{L/K}(\alpha)$ は共に K の元で，

$$Tr_{L/K}(\alpha+\beta) = Tr_{L/K}(\alpha) + Tr_{L/K}(\beta)$$
$$N_{L/K}(\alpha\cdot\beta) = N_{L/K}(\alpha)\cdot N_{L/K}(\beta)$$

を満たす．また補題 4.3 の証明より，$L \supset M \supset K$ を有限次分離拡大とすると，

$$Tr_{L/K}(\alpha) = Tr_{M/K}\{Tr_{L/M}(\alpha)\}$$
$$N_{L/K}(\alpha) = N_{M/K}\{N_{L/M}(\alpha)\}$$

を満たすこともわかる．

例 7.1　$K=\boldsymbol{Q}$, $L=\boldsymbol{Q}(\sqrt{d})$（$d\in\boldsymbol{Z}$ は非平方数）とし，$\alpha=a+b\sqrt{d}$（$a,b\in\boldsymbol{Q}$）とする．このとき

$$Tr_{L/K}(\alpha) = (a+b\sqrt{d}) + (a-b\sqrt{d}) = 2a$$
$$N_{L/K}(\alpha) = (a+b\sqrt{d})\cdot(a-b\sqrt{d}) = a^2-b^2d$$

となる．したがって，$N_{L/K}(a+b\sqrt{d}) = a^2-b^2d$ は a,b についての 2 次式となり，逆に a,b についての $\boldsymbol{Q}$-係数の既約な 2 次式は，適当な体 $L=\boldsymbol{Q}(\sqrt{d})$ をとると変数 a,b の 1 次変換の差を除き $N_{L/K}(a+b\sqrt{d})$ の形となる．

7.2　同型写像の 1 次独立性

補題 7.2　（アルティン）　$\chi_1,\chi_2,\cdots,\chi_m$ を半群 S から体 K の乗法群への相異なる準同型とする．このとき，$a_1,a_2,\cdots,a_m\in K$ がすべての $s\in S$ に対し

$$a_1\chi_1(s) + a_2\chi_2(s) + \cdots + a_m\chi_m(s) = 0$$

を満たすなら，$a_1=a_2=\cdots=a_m=0$ となる．

［証明］　そうでないものとし，上式を満たす $a_1,a_2,\cdots,a_m$ ですべては 0 ではないもののうち，m が最小のものをとる．

最小性より $a_1 \neq 0$ である．また $m=1$ なら $a_1\chi_1(s)=0$, $\chi_1(s)\neq 0$ より $a_1=0$ となり矛盾する．よって $m \geqq 2$ である．

補題の式の s に ts を代入し，準同型であることを使うと，

$$a_1\chi_1(t)\chi_1(s)+a_2\chi_2(t)\chi_2(s)+\cdots+a_m\chi_m(t)\chi_m(s)=0$$

となる．他方補題の式に $\chi_m(t)$ を掛けたものを作り，この式から引くと，

$$a_1(\chi_1(t)-\chi_m(t))\chi_1(s)+a_2(\chi_2(t)-\chi_m(t))\chi_2(s)+\cdots$$
$$+a_{m-1}(\chi_{m-1}(t)-\chi_m(t))\chi_{m-1}(s)=0$$

となる．仮定より $\chi_1 \neq \chi_m$ だから，適当な $t\in S$ をとると $\chi_1(t)\neq\chi_m(t)$ となる．そこで $b_i=a_i(\chi_i(t)-\chi_m(t))\in K$ とおくと，$b_1\neq 0$ かつ任意の $s\in S$ に対し，

$$b_1\chi_1(s)+b_2\chi_2(s)+\cdots+b_{m-1}\chi_{m-1}(s)=0$$

が成り立ち，mの最小性に矛盾する． （証明終）

補題において，χ_i として体の同型をとると，次の定理を得る．

定理 7.3 （デデキンド） $\sigma_1,\sigma_2,\cdots,\sigma_m$ を体 K から体 K' への相異なる同型とする．このとき，$a_1,a_2,\cdots,a_m\in K'$ が任意の $\theta\in K$ に対し，

$$a_1\sigma_1(\theta)+a_2\sigma_2(\theta)+\cdots+a_m\sigma_m(\theta)=0$$

を満たすなら，$a_1=a_2=\cdots=a_m=0$ となる．

L/K を m 次分離拡大とし，$\bar{K}$ を L を含む K の代数的閉包，$\sigma_1,\sigma_2,\cdots,\sigma_m$ を $L\longrightarrow\bar{K}$ なる K–同型の全体とする．このとき，$a_1,a_2,\cdots,a_m\in\bar{K}$ がすべては 0 でないなら，定理 7.3 より，適当な $\theta\in L$ に対し，

$$a_1\sigma_1(\theta)+a_2\sigma_2(\theta)+\cdots+a_m\sigma_m(\theta)\neq 0$$

となる．そこで $L\ni\beta\neq 0$ をとり，$a_i=\sigma_i(\beta)$ とおくと，適当な $\theta=\alpha\in L$ に対し，

$$Tr_{L/K}(\alpha\beta)=\sigma_1(\beta)\sigma_1(\alpha)+\sigma_2(\beta)\sigma_2(\alpha)+\cdots+\sigma_m(\beta)\sigma_m(\alpha)\neq 0$$

となることがわかる．これより，

系 7.4 L/K を有限次分離拡大とするとき，$T(\alpha,\beta)=Tr_{L/K}(\alpha\beta)$ は $L\times L\longrightarrow K$ なる非退化双 1 次形式を与える．

[証 明] 双 1 次形式であることは，トレースの定義より明らかである．非退化なこと

は既に示した．　(証明終)

7. 3 ヒルベルトの定理 90　L/K を有限次ガロア拡大とし，そのガロア群を G とする．このとき，L の乗法群 $L^* = L\setminus\{0\}$ には G が作用する．したがって，L^* は G の群環 $\boldsymbol{Z}[G]$ 上の加群となる．そこで，第Ⅳ章，例 4.8 の意味でのコホモロジー $H^n(G, L^*) = \mathrm{Ext}_{\boldsymbol{Z}[G]}{}^n(\boldsymbol{Z}, L^*)$ を考え，これを L^* の**ガロア·コホモロジー**とよぶ．

第Ⅳ章，例 4.8 より，

$$\mathrm{Hom}_{\boldsymbol{Z}[G]}(P_n, L^*) = \{f : G^n \longrightarrow L^*\}$$

($n=0$ のときは L^* とみなす) において，

$$(\delta^n f)(\sigma_1, \sigma_2, \cdots, \sigma_{n+1}) = \sigma_1\{f(\sigma_2, \cdots, \sigma_{n+1})\}$$
$$\cdot\{\prod_{1\leqq i\leqq n} f(\sigma_1, \cdots, \sigma_i\sigma_{i+1}, \cdots, \sigma_{n+1})^{(-1)^i}\}\cdot f(\sigma_1, \cdots, \sigma_n)^{(-1)^{n+1}}$$

で複体写像を定め，その複体のホモロジーを $H^n(G, L^*)$ とすればよい．したがって，

$$H^0(G, L^*) = \{f\in L^* \mid \sigma(f)/f = 1 \ \ (\forall\sigma\in G)\}$$
$$= \{f\in L^* \mid \sigma(f) = f \ (\forall\sigma\in G)\} = K^*$$

である．また

$$\mathrm{Ker}(\delta^1) = \{f : G\longrightarrow L^* \mid \sigma\{f(\tau)\}f(\sigma\tau)^{-1}f(\sigma) = 1 \ (\forall\sigma, \tau\in G)\}$$
$$= \{f : G\longrightarrow L^* \mid f(\sigma\tau) = \sigma\{f(\tau)\}f(\sigma) \ \ (\forall\sigma, \tau\in G)\},$$
$$\mathrm{Im}(\delta^0) = \{f : G\longrightarrow L^* \mid \text{ある } \gamma\in L^* \text{ に対し}$$
$$f(\sigma) = \sigma(\gamma)/\gamma \ \ (\forall\sigma\in G)\}$$

なる表現を使い，

$$H^1(G, L^*) = \mathrm{Ker}(\delta^1)/\mathrm{Im}(\delta^0)$$

が計算される．

定理 7. 5　(ヒルベルトの定理 90)　L/K を有限次ガロア拡大とし，そのガロア群を G，L の乗法群を L^* とすると，$H^1(G, L^*) = 0$ が成り立つ．

[証 明] $f : G \longrightarrow L^*$ が $f(\sigma\tau) = \sigma\{f(\tau)\}f(\sigma)$ $(\forall\sigma, \tau \in G)$ を満たすとする．このとき，任意の $\theta \in L$ に対し，

$$\sigma\{\sum_{\tau\in G} f(\tau)\tau(\theta)\}f(\sigma) = \sum_{\tau\in G} f(\sigma\tau)(\sigma\tau)(\theta) = \sum_{\tau\in G} f(\tau)\tau(\theta)$$

が成り立つ．ところが，定理 7.3 より，適当な $\theta \in L$ をとると，

$$\sum_{\tau\in G} f(\tau)\tau(\theta) \neq 0$$

とできる．これを γ^{-1} とおくと，$f(\sigma) = \sigma(\gamma)/\gamma$ となり，$f \in \mathrm{Im}(\delta^0)$ となる．

(証明終)

L/K，G を定理の通りとし，$\chi : G \longrightarrow K^*$ を群の準同型とする． このとき $\chi \in \mathrm{Ker}(\delta^1)$ となるから，定理より，

系 7. 6 L/K，G を定理の通りとし，$\chi : G \longrightarrow K^*$ を群の準同型とする．このとき $\gamma \in L^*$ を適当にとると，$\chi(\sigma) = \sigma(\gamma)/\gamma$ $(\forall\sigma \in G)$ と書ける．

また次も成り立つ．

系 7. 7 L/K を有限次巡回拡大とし，σ を $\mathrm{Gal}(L/K)$ の生成元とする．このとき $N_{L/K}(\alpha) = 1$ なる元 $\alpha \in L^*$ は，$\alpha = \sigma(\beta)/\beta$ $(\beta \in L^*)$ の形に表される．

[証 明] $f(1) = 1, \quad f(\sigma^i) = \alpha\sigma(\alpha)\cdots\sigma^{i-1}(\alpha) \quad (i \geqq 1)$

とおく．$[L : K] = n$ なら $f(\sigma^n) = N_{L/K}(\alpha) = 1$ となり，f は $\mathrm{Ker}(\delta^1)$ の元を与える．よって定理により，適当な $\beta \in L^*$ をとると，$f(\sigma^i) = \sigma^i(\beta)/\beta$ と書ける．とくに $\alpha = f(\sigma) = \sigma(\beta)/\beta$ となる．(証明終)

(注) 定理における L の乗法群 L^* を L の加法群でおき換え，同様の議論を行うと，

$$H^0(G, L) = K, \qquad H^n(G, L) = 0 \qquad (n \geqq 1)$$

が成り立つことがわかる．したがって，系 7.6，系 7.7 において，乗法を加法に直した形の結果も成り立つ．

問 題 7. 8 L/K を有限次巡回拡大，$\alpha \in L$ とする．このとき，$Tr_{L/K}(\alpha) = 0$ なら $\alpha = \sigma(\beta) - \beta$ $(\beta \in L)$ と書けることを示せ．

§8.　代数方程式の代数的可解性

8.1　巡回拡大　§7のヒルベルトの定理90を使うと，m 次巡回拡大 L/K において，K が1の原始 m 乗根を含むなら，L は次の様な形で与えられることがわかる．

定理 8.1　K を原始 m 乗根 ζ を含む体とする．このとき，次の (1), (2) が成り立つ．

(1)　$a \in K^* = K \setminus \{0\}$ に対し，$x^m - a = 0$ の1根を $\sqrt[m]{a}$ で表し，$L = K(\sqrt[m]{a})$, $d = [L:K]$ とおく．このとき，L/K は巡回拡大で，$d|m$, $(\sqrt[m]{a})^l \notin K$ $(1 \leqq l < d)$, $(\sqrt[m]{a})^d \in K$ である．

(2)　$d|m$ とし，L/K を d 次巡回拡大とする．このとき適当な $a \in K^*$ をとると，$L = K(\sqrt[m]{a})$ と書ける．

[証明]　K は原始 m 乗根を含むから，命題6.2より，K の標数は m と素である．したがって，$d|m$ なら，K の d 次拡大は分離的である．

(1)　$\theta = \sqrt[m]{a}$ とおく．θ は $x^m - a = \prod_{0\leq i<m}(x - \zeta^i\theta)$ の根だから，θ の K 上の共役は $\zeta^i\theta$ $(0 \leqq i < m)$ の形である．したがって，$\zeta^i\theta \in L$ だから，L/K は正規である．そこで，L/K のガロア群を G とおく．このとき，$G \ni \sigma$ に対し $\sigma(\theta) = \zeta^{i(\sigma)}\theta$ $(0 \leqq \exists i(\sigma) < m)$ と書き，

$$G = \mathrm{Gal}(L/K) \ni \sigma \longmapsto i(\sigma) \pmod{m} \in \boldsymbol{Z}/m\boldsymbol{Z}$$

なる写像を定める．$\zeta \in K$ だから，これは群の準同型である．また $L = K(\theta)$ だから，これは単射である．したがって，G は $\boldsymbol{Z}/m\boldsymbol{Z}$ の部分群と同型となるから，$d = [L:K] = \# G$ は m の約数である．また巡回群の部分群は巡回群だから，位数を考えると $i(G) = (m/d)\boldsymbol{Z}/m\boldsymbol{Z}$ となる．したがって，

$$\sigma(\theta^l) = \zeta^{li(\sigma)}\theta^l$$

より，$\theta^l \notin K$ $(1 \leqq l < d)$, $\theta^d \in K$ が成り立つ．

(2)　L/K を d 次巡回拡大で，$d|m$ とし，G をそのガロア群，σ を G の生成元とする．必要なら ζ を $\zeta^{m/d}$ でおき直すことにより，$d = m > 1$ と仮定してよい．

$N_{L/K}(\zeta) = \zeta^m = 1$ だから，ヒルベルトの定理90により，$\zeta = \sigma(\beta)/\beta$ となる $\beta \in L^*$

が存在する．このとき，$\sigma(\beta)=\zeta\beta$ だから，$\sigma^i(\beta)=\zeta^i\beta$ $(0\leqq i<m)$ はすべて相異なる．したがって，$L\supset K(\beta)$ かつ

$$m=[L:K]\geqq[K(\beta):K]\geqq[K(\beta):K]_s\geqq m$$

が成り立つから，$L=K(\beta)$ である．ここで，$\sigma(\beta^m)=\zeta^m\beta^m=\beta^m$ だから，$a=\beta^m\neq 0$ は K の元である．よって $L=K(\sqrt[m]{a})$ $(a\in K^*)$ と書ける．　　　　（証明終）

系 8.2　K を1の原始 m 乗根を含む体とする．このとき，$L=K(\sqrt[m]{a_1},\sqrt[m]{a_2},\cdots,\sqrt[m]{a_r})$ $(a_1,a_2,\cdots,a_r\in K^*)$ は K の有限次アーベル拡大で，そのガロア群の各元は $\sigma^m=1$ を満たす．逆に，L/K が有限次アーベル拡大で，そのガロア群の各元が $\sigma^m=1$ を満たすなら，$L=K(\sqrt[m]{a_1},\sqrt[m]{a_2},\cdots,\sqrt[m]{a_r})$ $(a_1,a_2,\cdots,a_r\in K^*)$ と書ける．このような拡大 L/K を，**m-クンマー拡大**という．

［証 明］　$L_i=K(\sqrt[m]{a_i})$ とおくと，定理より，L_i/K は $d_i=[L_i:K]$ 次の巡回拡大で，$d_i|m$ である．よって，$\tau\in\mathrm{Gal}(L_i/K)$ は $\tau^m=1$ を満たす．ところが $L=L_1\cdot L_2\cdots L_r$ だから，L/K はガロア拡大で，準同型写像

$$\begin{aligned}\mathrm{Gal}(L/K)\ni\sigma\ \longmapsto\ &(\sigma|_{L_1},\sigma|_{L_2},\cdots,\sigma|_{L_r})\\ &\in\mathrm{Gal}(L_1/K)\times\mathrm{Gal}(L_2/K)\times\cdots\times\mathrm{Gal}(L_r/K)\end{aligned}$$

は単射である．よって L/K はアーベル拡大で，$\sigma\in\mathrm{Gal}(L/K)$ は $\sigma^m=1$ を満たす．

逆に L/K がアーベル拡大で，$G=\mathrm{Gal}(L/K)$ の各元が $\sigma^m=1$ を満たすとする．G は有限アーベル群だから，第II章，定理6.2により，

$$G=G_1\times G_2\times\cdots\times G_r,\qquad G_i\simeq \boldsymbol{Z}/d_i\boldsymbol{Z},\ d_i|m$$

と書ける．そこで　$G_1\times\cdots\times G_{i-1}\times G_{i+1}\times\cdots\times G_r$　による不変体を L_i とおくと，

$$L=L_1\cdot L_2\cdots L_r,\qquad \mathrm{Gal}(L_i/K)\simeq\boldsymbol{Z}/d_i\boldsymbol{Z}$$

が成り立つ．よって定理8.1より，$L_i=K(\sqrt[m]{a_i})$ $(a_i\in K^*)$ と書け，$L=L_1\cdot L_2\cdots L_r$ は系の形になる．　　　　（証明終）

8.2　代数的可解性　　K を標数0の体とする．L/K を有限次拡大とするとき，

$$K=L_0\subset L_1\subset\cdots\subset L_r=L,\qquad L_i=L_{i-1}(\sqrt[m_i]{a_i})$$
$$(a_i\in L_{i-1},\ m_i\in\boldsymbol{N})$$

なる列があるとき，L/K は**べき根による拡大**であるという．ここで $\sqrt[m_i]{a_i}$ は $x^{m_i}-a_i=0$ の適当な1根とする．

$$f(x)=a_nx^n+a_{n-1}x^{n-1}+\cdots+a_1x+a_0\in K[x]$$

とし，$f(x)$ の K 上の分解体を M とする．このとき，M を含む K の有限次のべき根による拡大が存在するなら，方程式 $f(x)=0$ は K 上で**代数的に解ける**という．このことは，$f(x)=0$ の根すべてが，K の元に四則演算とべき根をとるという操作を有限回繰り返して得られることを意味する．例えば，2次方程式

$$ax^2+bx+c=0$$

は，その根が

$$x=(-b\pm\sqrt{b^2-4ac})/2a\ \in\ \boldsymbol{Q}(a,b,c)(\sqrt{b^2-4ac})$$

となるから，$\boldsymbol{Q}(a,b,c)$ 上代数的に解ける．

定理 8.3 上の意味で，方程式 $f(x)=0$ が K 上で代数的に解けるための必要十分条件は，$f(x)\in K[x]$ の K 上の分解体が，K の可解拡大（202ページおよび第II章，8.3参照）となることである．

［証明］ $f(x)$ の K 上の分解体を M, $G=\mathrm{Gal}(M/K)$ とする．

（必要性） M を含む K のべき根による拡大 L をとり，

$$K=L_0\subset L_1\subset\cdots\subset L_r,\qquad L_i=L_{i-1}(\sqrt[m_i]{a_i})\qquad(a_i\in L_{i-1})$$

を対応する列とする．$m=m_1m_2\cdots m_r$ とし，K に1の原始 m 乗根 ζ を添加した体を $K'=K(\zeta)$ とする．定理6.4より K' は K のアーベル拡大である．また $L_1'=K'\cdot L_1$ は $K'(\sqrt[m_1]{a_1})$ $(a_1\in K)$ の形であり，K' は1の原始 m_1 乗根を含むから，L_1' は K の正規拡大で，L_1'/K' は巡回拡大となる．次に a_2 の K 上の共役全体を $a_2,a_2',a_2'',\cdots$ とし，$L_2'=L_1'(\sqrt[m_2]{a_2},\ \sqrt[m_2]{a_2'},\ \sqrt[m_2]{a_2''},\cdots)$ とおく．L_1' は1の原始 m_2 乗根を含むから，L_2' は K の正規拡大で，系8.2より L_2'/L_1' はアーベル拡大である．以下帰納的に，a_i の K 上の共役全体を $a_i,a_i',a_i'',\cdots$ とし，$L_i'=L_{i-1}'(\sqrt[m_i]{a_i},\ \sqrt[m_i]{a_i'},\ \sqrt[m_i]{a_i''},\cdots)$ とおく．このとき，L_i' は K の正規拡大で，L_i'/L_{i-1}' はアーベル拡大となる．とくに L_r' は K の正規拡大となる．K の標数は0だから，L_r' は K の有限次ガロア拡大である．G' を L_r'/K のガロア群とし，L_i' に対する部分群を G_i' とすると，

$$G' \supset G_0' \supset G_1' \supset \cdots \supset G_r' = \{1\},$$

$$G' \triangleright G_i',\ G_{i-1}'/G_i' \simeq \mathrm{Gal}(L_i'/L_{i-1}') \text{ はアーベル群}$$

となる．したがって G' は可解群である．

M は L' の部分体で K 上正規である．よって，$\mathrm{Gal}(L'/M)$ は G' の正規部分群で，$G = \mathrm{Gal}(M/K) \simeq \mathrm{Gal}(L'/K)/\mathrm{Gal}(L'/M)$ である．ところが，可解群の商群は可解群だから，G は可解群である（第Ⅱ章，命題 8.16 参照）．

（十分性） M/K が可解拡大だとする．$m = [M:K]$ とし，K に 1 の原始 m 乗根 ζ を添加した体を $K' = K(\zeta)$ とする．このとき，$M' = K' \cdot M$ は K' の可解拡大で，$[M':K'] \mid [M:K] = m$ である．$G' = \mathrm{Gal}(M'/K')$ は可解群だから，

$$G' \supset G_1' \supset G_2' \supset \cdots \supset G_r' = \{1\}, \qquad G_{i-1}' \triangleright G_i',\ G_{i-1}'/G_i' \text{ は巡回群}$$

となる列が存在する．そこで，M'/K' の中間体で，G_i' に対応するものを L_i とおく．このとき，

$$K \subset K' \subset L_1 \subset L_2 \subset \cdots \subset L_r = K' \cdot M$$

なる列において，L_i は L_{i-1} のガロア拡大で，$\mathrm{Gal}(L_i/L_{i-1}) \simeq G_{i-1}'/G_i'$ は巡回群である．この群の位数は m の約数で，$L_{i-1} \supset K'$ は 1 の原始 m 乗根を含むから，定理 8.1 より，$L_i = L_{i-1}(\sqrt[m_i]{a_i})$ （$\exists a_i \in L_i$）と書ける．よって $L = L_r$ は K のべき根による拡大で，$f(x)$ の分解体 M を含む． （証明終）

8.3 n 次の一般方程式 k を標数 0 の体とし，文字 $a_{n-1}, a_{n-2}, \cdots, a_1, a_0$ についての有理関数体を $K = k(a_{n-1}, a_{n-2}, \cdots, a_1, a_0)$ とする．このとき，K に係数をもつ方程式

$$f(x) = x^n - a_{n-1}x^{n-1} + \cdots + (-1)^{n-1}a_1x + (-1)^n a_0 = 0$$

を，k 上の **n 次の一般方程式** とよぶ．

この方程式の根を $\theta_1, \theta_2, \cdots, \theta_n$ とすると，根と係数の関係より，係数 $a_{n-1}, a_{n-2}, \cdots, a_1, a_0$ は

$$a_{n-i} = s_i(\theta_1, \theta_2, \cdots, \theta_n) \qquad (i = 1, 2, \cdots, n-1, n)$$

と $\theta_1, \theta_2, \cdots, \theta_n$ の基本対称式として書ける（例 5.8 参照）．

定理 8.4 n 次一般方程式 $f(x) = 0$ の K 上のガロア群は，対称群 S_n と同型である．

［証明］ 文字 $a_{n-1}, a_{n-2}, \cdots, a_0$ についての多項式環 $k[a_{n-1}, a_{n-2}, \cdots, a_0]$ から，文字 $x_1, x_2, \cdots, x_n$ の基本対称式

$$s_i = s_i(x_1, x_2, \cdots, x_n) \in k[x_1, x_2, \cdots, x_n]$$

の生成する環 $k[s_1, s_2, \cdots, s_n]$ への準同型写像 ι を，

$$\iota: \quad k[a_{n-1}, a_{n-2}, \cdots, a_0] \ni g(a_{n-1}, a_{n-2}, \cdots, a_0)$$
$$\longmapsto \quad g(s_1, s_2, \cdots, s_n) \in k[s_1, s_2, \cdots, s_n]$$

で定義する．これは明らかに全射である．また $g(s_1, s_2, \cdots, s_n) = 0$ なら，文字 x_i に θ_i を代入すると，

$$\begin{aligned} g(a_{n-1}, a_{n-2}, \cdots, a_0) &= g(s_1(\theta_1, \theta_2, \cdots, \theta_n), s_2(\theta_1, \theta_2, \cdots, \theta_n), \cdots, s_n(\theta_1, \theta_2, \cdots, \theta_n)) \\ &= 0 \end{aligned}$$

となる．よって ι は環の同型である．したがって，ι は商体の同型 $\iota' : K = k(a_{n-1}, a_{n-2}, \cdots, a_0) \simeq k(s_1, s_2, \cdots, s_n)$ をひきおこす．この同型により，$f(x) \in K[x]$ は

$$x^n - s_1 x^{n-1} + \cdots + (-1)^{n-1} s_{n-1} x + (-1)^n s_n = (x - x_1)(x - x_2)\cdots(x - x_n)$$

に写される．したがって，例 5.8 より，

$$\mathrm{Gal}(k(\theta_1, \theta_2, \cdots, \theta_n)/k(a_{n-1}, a_{n-2}, \cdots, a_0)) \simeq \mathrm{Gal}(k(x_1, x_2, \cdots, x_n)/k(s_1, s_2, \cdots, s_n))$$

は対称群 S_n と同型になる． （証明終）

第Ⅱ章，§8 により，対称群 S_n は $n \leqq 4$ のときに限り可解群となる．したがって，定理 8.3 と定理 8.4 より，次のことがわかる．

系 8.5 （アーベル） n 次の一般方程式がべき根のみにより解けるための必要十分条件は，$n \leqq 4$ なることである．

例 8.6 $f(x) = x^n - a_{n-1}x^{n-1} + \cdots + (-1)^{n-1}a_1 x + (-1)^n a_0$
を体 K 上の n 次の多項式とし，その根を $\theta_1, \theta_2, \cdots, \theta_n$ とする．このとき θ の差積 $\prod_{i<j}(\theta_i - \theta_j)$ は，$\{\theta_1, \theta_2, \cdots, \theta_n\}$ の置換を行ったとき，奇置換なら符号が変り，偶置換なら不変である．したがって，

$$D(f) = \prod_{i<j}(\theta_i - \theta_j)^2$$

は根 $\{\theta_1, \theta_2, \cdots, \theta_n\}$ の置換で不変だから，K の元となる．これを，f の **判別式** という．

$f(x)$ が体 k 上の n 次一般方程式で，$K = k(a_{n-1}, \cdots, a_1, a_0)$ だとする．このとき，$L = K(\theta_1, \theta_2, \cdots, \theta_n)$ は $f(x)$ の K 上の分解体で，$\mathrm{Gal}(L/K) \simeq S_n$ である．よって上の議

論より，$D(f) \in K$，かつ $M = K(\sqrt{D(f)})$ $(\sqrt{D(f)} = \prod_{i<j}(\theta_i - \theta_j))$ は S_n の部分群 A_n に対応する K の拡大であることがわかる．

例 8.7　$f(x) \in K[x]$ の K 上のガロア群が可解群となるときは，$f(x)$ の任意の根を $f(x)$ の係数のべき根を含む式として表すことが，定理 8.3 の十分性の証明を具体的に行うことによりできる．この場合，途中で使った系 7.7（または定理 7.5）の解を捜す部分にのみ，多少の工夫がいる．このことを，3 次の一般方程式

$$f(x) = x^3 + a_2x^2 + a_1x + a_0 \in k[a_2, a_1, a_0][x]$$

について，実際に実行すると，次のようになる：

$K = k(a_2, a_1, a_0)$ とし，L を $f(x)$ の分解体とする．$y = x + (a_2/3)$ とおくと，$f(x)$ は

$$g(y) = y^3 + py + q \qquad (p, q \text{ は } a_2, a_1, a_0 \text{ の多項式})$$

の形となる．$g(y) = 0$ の 3 根を $\theta_1, \theta_2, \theta_3$ とする．

$g(y)$ の判別式 $D(g)$ は，$\theta_1 + \theta_2 + \theta_3 = 0$ に注意すると，

$$\begin{aligned} D(g) &= (\theta_1 - \theta_2)^2(\theta_1 - \theta_3)^2(\theta_2 - \theta_3)^2 \\ &= -4(\theta_1\theta_2 + \theta_2\theta_3 + \theta_3\theta_1)^3 - 27(\theta_1\theta_2\theta_3)^2 = -4p^3 - 27q^2 \end{aligned}$$

と計算できる．そこで，$M = K(\sqrt{D(g)})$ とおくと，M は S_3 の部分群 $A_3 = \langle(1, 2, 3)\rangle$ に対する L/K の部分体で，L/M は 3 次の巡回拡大となる．

$\omega = (-1 + \sqrt{-3})/2$ なる 1 の原始 3 乗根をとり，ヒルベルトの定理 90 の証明を参考にし，

$$\begin{aligned} \xi_1 &= \theta_1 + \theta_2 + \theta_3 = 0 \\ \xi_2 &= \theta_1 + \omega\theta_2 + \omega^2\theta_3 \\ \xi_3 &= \theta_1 + \omega^2\theta_2 + \omega\theta_3 \end{aligned}$$

を考える．これらは $L(\omega)$ の元だが，$G = \mathrm{Gal}(L(\omega)/M(\omega)) \simeq \mathrm{Gal}(L/M) \simeq A_3$ の生成元 $\sigma = (1, 2, 3)$ により，

$$\sigma(\xi_2) = \omega\xi_2, \qquad \sigma(\xi_3) = \omega^2\xi_3$$

と動く．よって $\xi_2{}^3, \xi_3{}^3, \xi_2\xi_3$ は $M(\omega)$ に属す．実際 $\xi_2{}^3, \xi_3{}^3$ は，

$$\begin{aligned} \xi_2{}^3 &= \frac{27}{2}(\theta_1\theta_2\theta_3) + \frac{3}{2}\sqrt{-3}(\theta_1 - \theta_2)(\theta_1 - \theta_3)(\theta_2 - \theta_3) \\ &= -\frac{27}{2}q + \frac{3}{2}\sqrt{-3}\sqrt{D(g)} \end{aligned}$$

$$\xi_3{}^3 = \frac{27}{2}(\theta_1\theta_2\theta_3) - \frac{3}{2}\sqrt{-3}\,(\theta_1-\theta_2)(\theta_1-\theta_3)(\theta_2-\theta_3)$$

$$= -\frac{27}{2}q - \frac{3}{2}\sqrt{-3}\sqrt{D(g)}$$

となり，$M(\omega) = K(\omega, \sqrt{D(g)})$ に属す．また

$$\xi_2\xi_3 = -3(\theta_1\theta_2 + \theta_2\theta_3 + \theta_3\theta_1) = -3p$$

となる．

そこで

$$\xi_2 = \sqrt[3]{-\frac{27}{2}q + \frac{3}{2}\sqrt{D(g)}}, \qquad \xi_3 = \sqrt[3]{-\frac{27}{2}q - \frac{3}{2}\sqrt{-3}\sqrt{D(g)}}$$

を，$\xi_2\xi_3 = -3p$ を満たす立方根の組とし，これより連立方程式

$$\begin{cases} \theta_1 + \theta_2 + \theta_3 = 0 \\ \theta_1 + \omega\theta_2 + \omega^2\theta_3 = \xi_2 \\ \theta_1 + \omega^2\theta_2 + \omega\theta_3 = \xi_3 \end{cases}$$

を $\theta_1, \theta_2, \theta_3$ について解くと，

$$\theta_1 = \frac{1}{3}(\xi_2 + \xi_3), \qquad \theta_2 = \frac{1}{3}(\omega^2\xi_2 + \omega\xi_3), \qquad \theta_3 = \frac{1}{3}(\omega\xi_2 + \omega^2\xi_3)$$

として3根が求まる．この公式は，カルダノにより求められた．

なお，4次方程式の根の公式も，$S_4 \supset A_4 \supset V \supset \{1\}$ なる正規列（第Ⅱ章，例8.10参照）を使うと，同様にして得られる．詳しくは，ファン・デル・ヴェルデン〔B7〕等を参照されたい．

§9. 代数的独立性

L/K を体の拡大とし，S を L の部分集合とする．このとき，S のある有限部分集合 $F = \{\theta_1, \theta_2, \cdots, \theta_n\}$ と適当な0でない多項式 $f(x_1, x_2, \cdots, x_n) \in K[x_1, x_2, \cdots, x_n]$ で，$f(\theta_1, \theta_2, \cdots, \theta_n) = 0$ となるものが存在するとき，S は K 上**代数的に従属**であるといい，そうでないとき，S は K 上**代数的に独立**であるという（§1参照）．

$F = \{\theta_1, \theta_2, \cdots, \theta_n\} \subset L$ が K 上代数的に独立なら，x_i に θ_i を代入して得られる環の準同型 $K[x_1, x_2, \cdots, x_n] \longrightarrow K[\theta_1, \theta_2, \cdots, \theta_n]$ は単射となり，よって

$K[x_1, x_2, \cdots, x_n] \simeq K[\theta_1, \theta_2, \cdots, \theta_n]$ となる．したがって，$K(F) = K(\theta_1, \theta_2, \cdots, \theta_n)$ は有理関数体 $K(x_1, x_2, \cdots, x_n)$ と同型となる．

拡大体 L/K が与えられたとき，L の部分集合 S で，S は K 上代数的に独立で，かつ L は体 $K(S)$ 上代数的となるものを L/K の **超越基底** とよぶ．とくに，L/K の超越基底 S で $L = K(S)$ となるものが存在するなら，L は K の **純超越拡大** であるという．L/K が純超越拡大なら，L は K 上の（一般には無限個の変数をもつ）有理関数体と同型となる．

定 理 9. 1 L/K を体の拡大とし，L は K 上部分集合 T により生成されるとする：$L = K(T)$．また S_0 を T の部分集合で，K 上代数的に独立であるとする．このとき，T の部分集合 $S \supset S_0$ で，L/K の超越基底となるものが存在する．さらに，拡大体 L/K が与えられたとき，L/K の超越基底の濃度は，超越基底のとり方によらずに一定である．この濃度を，L/K の **超越次数** とよび，trans. $\deg_K L$ と表す．

[証 明] $L = K(T)$，$S_0 \subset T$ を定理の通りとし，$S_0 \subset S \subset T$ かつ S は K 上代数的に独立となる S の全体 Σ を考える．Σ は T の部分集合として，包含関係により順序が入っている．しかも $S_0 \in \Sigma$ だから $\Sigma \neq \emptyset$ である．また Σ が帰納的順序集合であることも，代数的独立性の定義よりすぐわかる．よって Σ は極大元をもつ．そこでそれを S とおき，S が L/K の超越基底となることを示す．

もし S が L/K の超越基底でないなら，$L = K(T)$ は $K(S)$ 上代数的ではない．したがって，T の元 $t \in T$ で $K(S)$ 上代数的ではないものが存在する．$S^* = S \cup \{t\}$ とおく．もし S^* が代数的に従属なら，S^* の有限部分集合 $\{\theta_1, \theta_2, \cdots, \theta_n, t\}$ $(\theta_i \in S)$ と，0 でない多項式 $f(x_1, x_2, \cdots, x_n, x) \in K[x_1, x_2, \cdots, x_n, x]$ で，$f(\theta_1, \theta_2, \cdots, \theta_n, t) = 0$ となるものが存在する．これを x について整理して，

$$f(x_1, x_2, \cdots, x_m, x) = \sum_{0 \le i \le m} a_i(x_1, x_2, \cdots, x_n) x^i$$

$$(a_i(x_1, x_2, \cdots, x_n) \in K[x_1, x_2, \cdots, x_n], \quad a_m(x_1, x_2, \cdots, x_n) \neq 0)$$

の形に書く．$S \supset \{\theta_1, \theta_2, \cdots, \theta_n\}$ は K 上代数的に独立だから，$a_m(\theta_1, \theta_2, \cdots, \theta_n) \neq 0$ である．よって $f(\theta_1, \theta_2, \cdots, \theta_n, x) = \sum_i a_i(\theta_1, \theta_2, \cdots, \theta_n) x^i$ は $K(S)[x]$ の多項式として 0 でなく，$x = t$ を代入すると 0 となる．これは，t が $K(S)$ 上代数的ではないという仮定に

矛盾する．したがって $S^* = S \cup \{t\}$ は K 上代数的に独立となる．これは S の極大性に矛盾するから，$L = K(T)$ は $K(S)$ 上代数的になり，定理の前半が証明できた．

後半の証明は，簡単のため，L が K 上有限生成な場合に限り証明する．(一般の場合もツォルンの補題を使うと，同様に証明できる．) この場合，定理の前半より，L/K は有限個の元から成る超越基底をもつ．そこで $S = \{\theta_1, \theta_2, \cdots, \theta_n\}$ が L/K の超越基底で，L の有限部分集合 U が K 上代数的に独立なら，U は高々 n 個の元から成ることを示せば十分である．

$U = \{u_1, u_2, \cdots, u_l\}$ とする．このとき $S \cup \{u_1\}$ は K 上代数的に従属だから，K 上の $n+1$ 変数の多項式 f_1 で，$f_1(u_1, \theta_1, \theta_2, \cdots, \theta_n) = 0$ となるものが存在する．しかも仮定より，u_1 および $\theta_1, \theta_2, \cdots, \theta_n$ のうち少なくとも1つは，$f_1(u_1, \theta_1, \theta_2, \cdots, \theta_n)$ の中に本当に現れる．そこで $\{\theta_i\}$ の番号をつけ直し，u_1 と θ_1 は $f_1(u_1, \theta_1, \theta_2, \cdots, \theta_n)$ の中に本当に現れるとする．このとき，θ_1 は $K(u_1, \theta_2, \cdots, \theta_n)$ 上代数的となる．したがって，L は $K(u_1, \theta_2, \cdots, \theta_n)$ 上代数的となる．$\{\theta_i\}$ の番号を入れ替えながら，この操作を行うと，θ_2 と u_2, θ_3 と $u_3, \cdots$ が順に入れ替えられてゆく．そこでもし $l \gneqq n$ なら，L は $K(u_1, u_2, \cdots, u_n)$ 上代数的となり，とくに $u_{n+1}, u_{n+2}, \cdots$ は $K(u_1, u_2, \cdots, u_n)$ 上代数的となる．これは U が K 上代数的に独立だとの仮定に矛盾する．よって $l = \sharp U \leqq n$ となる．　(証明終)

問題 9.2　$K \subset M \subset L$ を体の拡大とする．もし L/M と M/K が有限生成なら

$$\text{trans.}\deg_K L = \text{trans.}\deg_K M + \text{trans.}\deg_M L$$

が成り立つことを示せ．

問題 9.3　K を体，$L = K(x)$ を K 上の1変数有理関数体とする．このとき，

$$\mathrm{Aut}(L/K) = \{x \longmapsto (ax+b)/(cx+d) \mid a, b, c, d \in K, ad - bc \neq 0\}$$

となることを示せ．

問　　題

1.　有限個の元からなる整域は，体となることを示せ．

2.　L/K を有限生成な体の拡大で，M をその中間体とする．このとき，M/K も有限生成となることを示せ．

(ヒント)　K をとり直し，M/K が代数的な場合に帰着させる．この場合，L/K の

超越基底を $\{x_1, x_2, \cdots, x_r\}$ とすると，

$$[M:K] \leqq [L:K(x_1, x_2, \cdots, x_r)] < \infty$$

が成り立つ．

3. L/K を正規拡大とし，$K[x]$ の既約多項式 $f(x)$ の $L[x]$ での素因数分解を，$f(x) = f_1(x)^{e_1} f_2(x)^{e_2} \cdots f_r(x)^{e_r}$ ($i \neq j$ なら $f_i(x) \neq f_j(x)$) とする．このとき，$e_1 = e_2 = \cdots = e_r$ で，$L[x]/f_i(x)$ はすべて K-同型であることを示せ．

4. K を標数 $p > 0$ の体，$\bar{K}$ を K の代数的閉包，

$$K^{p^{-\infty}} = \{\theta \in \bar{K} \mid \theta^{p^e} \in K \text{ なる } e \in \boldsymbol{N} \text{ が存在する}\}$$

とする．$K^{p^{-\infty}}$ は，K 上純非分離的な $\bar{K}$ の元全体からなる集合である．このとき，次のことを示せ．

（1） $\bar{K}/K$ の $\mathrm{Aut}(\bar{K}/K)$ による不変体は $K^{p^{-\infty}}$ である．

（2） $\bar{K}/K$ の中間体 M が完全体となるための必要十分条件は，$M \supset K^{p^{-\infty}}$ である．

（3） 完全体の代数拡大は完全体で，不完全体の有限次拡大は不完全体である．

5. K を標数 $p > 0$ の体，L/K を有限次拡大，L_s を L における K の分離閉包とし，e で $L^{p^e} \subset L_s$ となる最小の非負整数を表す．このとき，L/K が単拡大となるための必要十分条件は，

$$[L:K] = [L:K]_s p^e$$

が成り立つことである．

（注） L/K の中間体の個数が有限個であることも，必要十分条件となる．

6. x を $\boldsymbol{C}$ 上の超越元とし，$L = \boldsymbol{C}(x)$ とおく．2 以外の素数 p を固定し，$\zeta = \exp(2\pi i/p)$ とおく．$\sigma, \tau \in \mathrm{Aut}(L/\boldsymbol{C})$ を

$$\sigma(x) = \zeta x, \qquad \tau(x) = x^{-1}$$

で定め，σ, τ で生成される $\mathrm{Aut}(L/\boldsymbol{C})$ の部分群を G とおく．

（1） $\sigma^p = 1$，$\tau^2 = 1$，$\tau^{-1}\sigma\tau = \sigma^{-1}$ となることを示し，G が 2 面体群 D_p と同型であることを示せ．

（2） L における G の不変体を K とおく．$K = \boldsymbol{C}(x^p + x^{-p})$ であることを示せ．

（3） L/K の中間体をすべて求めよ．

7. $K = \boldsymbol{Q}$，$M = \boldsymbol{Q}(\sqrt{2}, \sqrt{3})$，$\theta = \sqrt{-(2+\sqrt{2})(3+\sqrt{6})}$，$L = M(\theta)$ とおく．このとき，L/K がガロア拡大であることを示せ．また，L/K のガロア群は，

$$\sigma : \sqrt{2} \longmapsto -\sqrt{2},\ \sqrt{3} \longmapsto \sqrt{3},\ \theta \longmapsto (\sqrt{2}-1)(\sqrt{3}-\sqrt{2})\theta$$

$$\tau : \sqrt{2} \longmapsto \sqrt{2},\ \sqrt{3} \longmapsto -\sqrt{3},\ \theta \longmapsto (\sqrt{3}-\sqrt{2})\theta$$

なる元で生成され，

$$\sigma^4 = \tau^4 = 1, \qquad \sigma\tau = \tau^3\sigma$$

なる基本関係式を持つ位数 8 の群（四元数群）であることを示せ．

8. $\zeta = \exp(2\pi\sqrt{-1}/17)$，$K = \boldsymbol{Q}$，$L = \boldsymbol{Q}(\zeta)$ とし，群 $U(\boldsymbol{Z}/17\boldsymbol{Z})$ の元 $\bar{a} = a \pmod{17}$ に対し，$\sigma_{\bar{a}}(\zeta) = \zeta^a$ で同型 $\iota : U(\boldsymbol{Z}/17\boldsymbol{Z}) \ni \bar{a} \longmapsto \sigma_{\bar{a}} \in \mathrm{Gal}(L/K)$ を定める（6.1 参照）．

（1）　$$U(\boldsymbol{Z}/17\boldsymbol{Z}) = \langle\bar{3}\rangle \supset \langle\bar{9}\rangle \supset \langle\overline{13}\rangle \supset \langle\overline{16}\rangle \supset \langle\bar{1}\rangle = \{1\}$$

が，アーベル群 $U(\boldsymbol{Z}/17\boldsymbol{Z})$ の組成列を与えることを示せ．

（2）$U(\boldsymbol{Z}/17\boldsymbol{Z}) \simeq \mathrm{Gal}(L/K)$ の部分群と，L/K の中間体とが，次のように対応することを示せ．

$\langle\bar{9}\rangle \longleftrightarrow \boldsymbol{Q}(\eta)$，$\eta = \zeta + \zeta^{-1} + \zeta^2 + \zeta^{-2} + \zeta^4 + \zeta^{-4} + \zeta^8 + \zeta^{-8}$

$\langle\overline{13}\rangle \longleftrightarrow \boldsymbol{Q}(\xi_0) = \boldsymbol{Q}(\xi_1)$，$\xi_0 = \zeta + \zeta^{-1} + \zeta^4 + \zeta^{-4}$，$\xi_1 = \zeta^3 + \zeta^{-3} + \zeta^5 + \zeta^{-5}$

$\langle\overline{16}\rangle \longleftrightarrow \boldsymbol{Q}(\lambda)$，$\lambda = \zeta + \zeta^{-1}$

（3）$\eta, \xi_0, \xi_1, \lambda$ が次の方程式を満たすことを示し，$\cos(2\pi/17) = \lambda/2$ が，$\boldsymbol{Q}$ 上 2 次方程式を何回か解くことにより求まることを示せ．

$$\eta^2 + \eta - 4 = 0, \qquad \xi_0{}^2 - \eta\xi_0 - 1 = 0, \qquad \xi_1{}^2 + (\eta+1)\xi_1 - 1 = 0,$$

$$\lambda^2 - \xi_0\lambda + \xi_1 = 0, \qquad \zeta^2 - \lambda\zeta + 1 = 0.$$

9. K を体，$f(x) \in K[x]$ を分離的多項式とし，方程式 $f(x) = 0$ の K 上のガロア群を G_f で表す．

（1）K の代数的閉包 $\bar{K}$ における $f(x)$ の根を $\alpha_1, \alpha_2, \cdots, \alpha_n$，$y_1, y_2, \cdots, y_n$ を K 上代数的に独立な元とし，

$$F(x) = \prod_{\sigma \in S_n} \{x - (\alpha_1 y_{\sigma(1)} + \alpha_2 y_{\sigma(2)} + \cdots + \alpha_n y_{\sigma(n)})\}$$

（S_n は n 次対称群）とおく．$F(x) \in R[y_1, y_2, \cdots, y_n][x]$ となることを示せ．

（2）　$$F(x) = F_1(x)F_2(x)\cdots F_r(x)$$

を，$K[y_1, y_2, \cdots, y_n][x]$ における既約多項式の積としての表示とする．ここで，$x - (\alpha_1 y_1 + \alpha_2 y_2 + \cdots + \alpha_n y_n)$ は $F_1(x)$ に含まれるものとする．このとき，$\sigma \in S_n$ で，$F_1(x)$ をそれ自身に移すもの全体のなす群は，G_f と同型なことを示せ．

（3） R を一意分解環，$\mathfrak{p}$ を R の素イデアル，K を R の商体，$\tilde{R} = R/\mathfrak{p}$ を剰余環とする．$f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0 \in R[x]$ は既約で，$f(x)$ の係数の $(\mathrm{mod}\ \mathfrak{p})$ をとってできる多項式 $\tilde{f}(x) \in \tilde{R}[x]$ は分離的であるとする．このとき，方程式 $\tilde{f}(x) = 0$ の $\tilde{R}$ の商体 $\tilde{K}$ 上でのガロア群 $G_{\tilde{f}}$ は，方程式 $f(x) = 0$ の K 上のガロア群 G_f の部分群とみなせることを示せ．

10. K を有限体とし，$f(x) \in K[x]$ は分離的だとする．$f(x) = f_1(x)f_2(x)\cdots f_r(x)$ を $K[x]$ での既約多項式の積としての表現とし，$d_i = \deg f_i(x)$ とおく．このとき，方程式 $f(x) = 0$ の K 上のガロア群は，その根の置換の群とみて，

$$(d_1\ \text{次巡回置換})(d_2\ \text{次巡回置換})\cdots(d_r\ \text{次巡回置換})$$

の型の置換で生成される巡回群であることを示せ．

11. $f(x) = x^5 - x - 1 \in \boldsymbol{Z}[x]$ とするとき，方程式 $f(x) = 0$ の $\boldsymbol{Q}$ 上のガロア群 G_f は，対称群 S_5 となることを示せ．さらに，任意の自然数 n に対し，$\boldsymbol{Q}$ のガロア拡大で，そのガロア群が S_n となるものが存在することを示せ．

（ヒント） $f(x)$ を $(\mathrm{mod}\ 2)$ と $(\mathrm{mod}\ 3)$ で既約因子に分解し，問題 9, (3)，問題 10，および第 II 章，問題 3.6 を使う．後半は前半を参考にする．

12. l を素数，K を原始 l 乗根 ζ を含む体，M を K の l^m 次巡回拡大とする．

（1） L を K の l^{m+1} 次の巡回拡大で M を含むものとする．$\mathrm{Gal}(L/K) = \langle\sigma\rangle$ とし，$a \in M$ で $(\sigma^{l^m})(\sqrt[l]{a}) = \zeta\sqrt[l]{a}$，$L = M(\sqrt[l]{a})$ なるものをとる．このとき $\sigma(\sqrt[l]{a}) = b(\sqrt[l]{a})^i$ $(b \in M,\ 1 \leqq i < l)$ と表せることを示せ．さらに $\sigma^{l^m}(\sqrt[l]{a})$ を計算し，$i^{l^m} \equiv 1 \pmod{l}$ となることより $i = 1$ を示し，これより $N_{M/K}(b) = \zeta$ が成り立つことを示せ．

（2） M の元 b で，$N_{M/K}(b) = \zeta$ なるものが存在したとする．$\mathrm{Gal}(M/K) = \langle\tau\rangle$ と表すとき $a \in M$ で $\tau(a)/a = b^l$ となるものが存在することを示せ．さらに，$L = M(\sqrt[l]{a})$ とおくとき，L/K が l^{m+1} 次巡回群となることを示せ．

（3） $\boldsymbol{Q}$ の 4 次巡回拡大で，$\boldsymbol{Q}(\sqrt{-d})$ $(d \in \boldsymbol{N}$ は平方数ではない）を含むものは存在しないことを示せ．

13. K を標数 $p > 0$ の体とする．次を示せ．

（1） $f(x) = x^p - x + a$ $(a \in K)$ が既約なら，K の上に $f(x) = 0$ の根 θ を添加してできる体 $L = K(\theta)$ は，K の p 次巡回拡大である．

(2) 逆に L/K が p 次巡回拡大なら，K はある既約な多項式 $f(x) = x^p - x + a$ $(a \in M)$ の根を，M に添加してできる．

(ヒント) L/K を p 次巡回拡大，$\mathrm{Gal}(L/K) = \langle\sigma\rangle$ とする．このとき，$\alpha \in L$ が $Tr_{L/K}(\alpha) = 0$ を満たすなら，$\alpha = \sigma(\beta) - \beta$ $(\beta \in L)$ と書ける．

14. (1) 次の体を含む最小の $\boldsymbol{Q}$ 上のガロア拡大を求め，そのガロア群を求めよ．

(a) $\boldsymbol{Q}(\sqrt{2})$,　(b) $\boldsymbol{Q}(\sqrt{3}+\sqrt{5})$,　(c) $\boldsymbol{Q}(\sqrt[4]{8})$.

(2) 次の拡大の中間体の個数を求めよ．

(d) $\boldsymbol{Q}(\sqrt{3}, \sqrt{5})/\boldsymbol{Q}$,　(e) $\boldsymbol{Q}(\sqrt{-1}, \sqrt[4]{8})/\boldsymbol{Q}$,　(f) $\boldsymbol{Q}(\sqrt[3]{5}, \sqrt[3]{7}, \sqrt[3]{11})/\boldsymbol{Q}$.

VI 圏 と 関 手*

Ⅱ章からⅤ章まで，群，環，加群，体などをとり上げ，個別に調べてきた．しかしその中には，準同型定理，同型などこれらの対象によらない共通するものがあった．このように，数学の対象を共通の言葉でとらえ，一般的に扱うための理論が，圏と関手である．

§1. 圏

群の全体を (Gr) で表すと，(Gr) の元 X, Y に対し，

$$\mathrm{Hom}(X, Y) = \{f : X \longrightarrow Y \mid \text{群の準同型}\}$$

という集合が定まり，$f \in \mathrm{Hom}(X, Y)$ と $g \in \mathrm{Hom}(Y, Z)$ に対し，$g \circ f \in \mathrm{Hom}(X, Z)$ が定まっている．

このように，数学的な **対象** の範囲 $\mathrm{Ob}(\mathscr{C})$ と，その範囲内の 2 つの対象 $X, Y \in \mathrm{Ob}(\mathscr{C})$ に対し，**射** とよばれるものの集合 $\mathrm{Hom}_{\mathscr{C}}(X, Y)$ が定められており，また，$f \in \mathrm{Hom}_{\mathscr{C}}(X, Y)$ と $g \in \mathrm{Hom}_{\mathscr{C}}(Y, Z)$ に対し，その **合成** とよばれる元 $g \circ f \in \mathrm{Hom}_{\mathscr{C}}(X, Z)$ が定められているものとする．このときさらに，これら $\mathrm{Ob}(\mathscr{C})$ と $\mathrm{Hom}_{\mathscr{C}}(X, Y)$ $(X, Y \in \mathrm{Ob}(\mathscr{C}))$ の集り $\mathscr{C}$ が次の 3 条件を満たすなら，$\mathscr{C}$ は **圏**（**カテゴリー**）をなすという：

(CT 1) $f \in \mathrm{Hom}_{\mathscr{C}}(X, Y)$, $g \in \mathrm{Hom}_{\mathscr{C}}(Y, Z)$, $h \in \mathrm{Hom}_{\mathscr{C}}(Z, W)$ のとき，$\mathrm{Hom}_{\mathscr{C}}(X, W)$ の元として，

$$(h \circ g) \circ f = h \circ (g \circ f)$$

が成り立つ．

(CT 2) 任意の $X \in \mathrm{Ob}(\mathscr{C})$ に対し，ある $1_X \in \mathrm{Hom}_{\mathscr{C}}(X, X)$ で，

$f \circ 1_X = f, \qquad 1_X \circ g = g \;\; (\forall f \in \mathrm{Hom}_{\mathscr{C}}(X, Y), \;\; \forall g \in \mathrm{Hom}_{\mathscr{C}}(Z, X))$

を満たすものが存在する．

(CT 3) (X, Y) と (X', Y') が相異なる $\mathscr{C}$ の対象の組なら，$\mathrm{Hom}_{\mathscr{C}}(X, Y)$ と $\mathrm{Hom}_{\mathscr{C}}(X', Y')$ は共通の元をもたない．

以下 $\mathscr{C}$ が明らかなときは，$\mathrm{Hom}_{\mathscr{C}}(X, Y)$ を $\mathrm{Hom}(X, Y)$ と略記する．また $X \in \mathrm{Ob}(\mathscr{C})$ のことを $X \in \mathscr{C}$ とも略記する．さらに，射 $f \in \mathrm{Hom}_{\mathscr{C}}(X, Y)$ のことを，$f : X \longrightarrow Y$ とも表す．

圏の定義においては，$\mathrm{Ob}(\mathscr{C})$ は必ずしも集合でなくてもよいが，$\mathrm{Ob}(\mathscr{C})$ が集合となるとき，$\mathscr{C}$ を **小さい圏** であるという．

$\mathscr{C}'$ が圏 $\mathscr{C}$ の **部分圏** であるとは，$\mathscr{C}'$ は圏であり，かつ次の 3 条件を満たすことをいう：

(SC 1) $\mathrm{Ob}(\mathscr{C}')$ の元は $\mathrm{Ob}(\mathscr{C})$ の元でもある．

(SC 2) 任意の $X, Y \in \mathscr{C}'$ に対し，$\mathrm{Hom}_{\mathscr{C}'}(X, Y)$ は $\mathrm{Hom}_{\mathscr{C}}(X, Y)$ の部分集合である．

(SC 3) $\mathscr{C}'$ における射の合成は，$\mathscr{C}$ における射とみての合成と一致する．

とくに，$X, Y \in \mathscr{C}'$ に対し，$\mathrm{Hom}_{\mathscr{C}'}(X, Y) = \mathrm{Hom}_{\mathscr{C}}(X, Y)$ が成り立つとき，$\mathscr{C}'$ は $\mathscr{C}$ の **充満部分圏** であるという．なお，圏 $\mathscr{C}$ の対象 X に対し，$\mathrm{Hom}_{\mathscr{C}}(X, X)$ は 1_X を単位元とする半群をなすから，$\mathscr{C}'$ が $\mathscr{C}$ の部分圏なら，1_X は $\mathscr{C}$ で考えても $\mathscr{C}'$ で考えても一致する．

例 1. 1 集合の全体を $\mathrm{Ob}(\mathscr{C})$ とし，集合としての写像を射とする圏を $\mathscr{C}$ とする．このとき，もし $\mathrm{Ob}(\mathscr{C})$ が集合なら，

$$X = \{x \in \mathrm{Ob}(\mathscr{C}) \mid x \notin x\}$$

を考えると，

$$x \in X \iff x \notin x$$

が成り立つ．よって，$X \in X$ でも $X \notin X$ でも，

$$X \in X \quad \text{かつ} \quad X \notin X$$

が成り立ち，矛盾である．よって Ob($\mathscr{C}$) は集合ではなく，$\mathscr{C}$ は小さい圏ではない．この $\mathscr{C}$ を，普通 (Sets) と表す．

例 1. 2　$\mathscr{C}_1$ を群の全体のなす圏，$\mathscr{C}_2$ をアーベル群全体のなす圏，$\mathscr{C}_3$ を可換環全体のなす圏とする．このとき，$\mathscr{C}_2$ は $\mathscr{C}_1$ の充満部分圏であり，$\mathscr{C}_3$ は $\mathscr{C}_2$ の部分圏をなす．しかし $X, Y \in \mathrm{Ob}(\mathscr{C}_3)$ のとき，一般には

$$\mathrm{Hom}_{\mathscr{C}_2}(X, Y) = \{f : X \longrightarrow Y \mid \text{加法群としての準同型}\}$$

は，

$$\mathrm{Hom}_{\mathscr{C}_3}(X, Y) = \{f : X \longrightarrow Y \mid \text{環の準同型}\}$$

より大きい．よって $\mathscr{C}_3$ は $\mathscr{C}_2$ の充満部分圏ではない．

例 1. 3　$\mathscr{C}$ を圏とするとき，Ob($\mathscr{C}$) を対象 Ob($\mathscr{C}^0$) とし，

$$\mathrm{Hom}_{\mathscr{C}^0}(X, Y) = \mathrm{Hom}_{\mathscr{C}}(Y, X)$$

を射の全体とすると，Ob($\mathscr{C}^0$) と $\mathrm{Hom}_{\mathscr{C}^0}(X, Y)$ の全体 ($\mathscr{C}^0$) は圏をなす．これを $\mathscr{C}$ の **双対圏** という．双対圏は，双対的な命題を扱うのに便利である．

圏 $\mathscr{C}$ が与えられたとき，$\mathscr{C}$ の射を使って，**可換図式** を考えることができる．

圏 $\mathscr{C}$ における射 $f : X \longrightarrow Y$ が **同型** であるとは，適当な射 $g : Y \longrightarrow X$ が存在し，$f \circ g = 1_Y$, $g \circ f = 1_X$ が成り立つこととする．このとき，$f : X \simeq Y$ または $X \simeq Y$ などと書き，X, Y は **同型** であるという．同型という関係は，同値関係をなす．

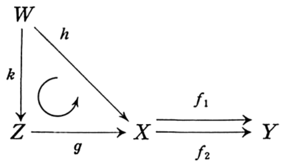
射 $f : X \longrightarrow Y$ が **単射** であるとは，任意の $\mathscr{C}$ の対象 Z と任意の射 $u, v : Z \longrightarrow X$ に対し，$u \neq v$ なら $f \circ u \neq f \circ v$ が成り立つこととする．同様にして，$f : X \longrightarrow Y$ が **全射** であるとは，任意の射 $u, v : Y \longrightarrow Z$ に対し，$u \neq v$ なら $u \circ f \neq v \circ f$ が成り立つこととする．同型は全射かつ単射であるが，逆は一般には成り立たない．

対象 X への 2 つの単射 $f_i : X_i \longrightarrow X\,(i = 1, 2)$ は，$f_1 = f_2 \circ g_1$, $f_2 = f_1 \circ g_2$ を満たす射　$g_1 : X_1 \longrightarrow X_2$, $g_2 : X_2 \longrightarrow X_1$　が存在するとき同値であるといい，この同値関係による類を，X の **部分対象** とよぶ．同様にして，X からの全射を分類して，**商対象** が定義される．

圏$\mathscr{C}$における対象eが，任意の$X\in \mathrm{Ob}(\mathscr{C})$に対し，$\mathrm{Hom}_{\mathscr{C}}(X,e)$が唯一つの元から成るなら，$e$は$\mathscr{C}$の**終対象**であるという．双対的に，$e'\in\mathscr{C}$が任意の$X\in \mathrm{Ob}(\mathscr{C})$に対し$\mathrm{Hom}_{\mathscr{C}}(e',X)$が唯一つの元から成るなら，$e'$は$\mathscr{C}$の**始対象**であるという．とくに，始対象かつ終対象となるものを**零対象**という．これらは存在すれば，同型の差を除き，一意的に定まる．

例 1.4　位相空間の圏では，連続な1対1の写像が単射であり，連続な上への写像が全射である．したがって，連続な1対1かつ上への写像が全単射であるが，この場合，逆写像の連続性はわからない．よって全単射でも同型となるとは限らない．

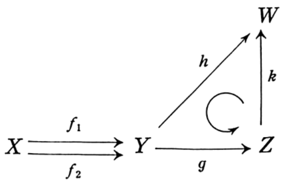
例 1.5　(単位元$1\neq 0$をもつ）環の圏では，整数のなす環$\boldsymbol{Z}$が始対象だが，終対象は存在しない．アーベル群の圏（$\boldsymbol{Z}$-加群の圏）では，$\{0\}$が零対象となる．



圏$\mathscr{C}$における射$f_1,f_2: X\longrightarrow Y$が与えられたとき，射$g: Z\longrightarrow X$で，次の2条件を満たすものを$f_1$と$f_2$の**差核**といい，$\mathrm{Ker}(f_1,f_2)$と表す：

(**K 1**)　　$f_1\circ g = f_2\circ g$,

(**K 2**)　$h: W\longrightarrow X$も$f_1\circ h=f_2\circ h$を満たすなら，$k: W\longrightarrow Z$で$h=g\circ k$なるものが唯一つ存在する．

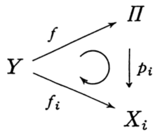


差核は必ずしも存在するとは限らないが，存在すればgは単射となり，ZはXの部分対象となる．双対的に，**双対差核**$\mathrm{Coker}(f_1,f_2)$も商対象として定義される．とくに，$\mathscr{C}$において零対象0が存在するときには，$\mathrm{Ker}(f,0)$を$\mathrm{Ker}(f)$と表し，**核**とよぶ．同様に，$\mathrm{Coker}(f,0)$を$\mathrm{Coker}(f)$と表し，**余核**とよぶ．後にのべるように，これらはアーベル圏では存在する．

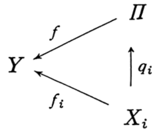
圏$\mathscr{C}$における対象の集合$\{X_i\}_{i\in I}$に対し，$\mathscr{C}$の対象Πと，$\mathscr{C}$での射の集合

$$p_i: \quad \Pi \longrightarrow X_i \qquad (i \in I)$$

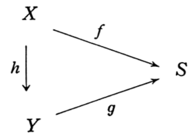
の組で，次の条件を満たすものを **直積** とよぶ：



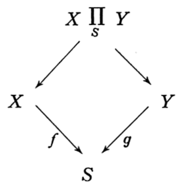
(P)　射の集合 $f_i: Y \longrightarrow X_i$ $(i \in I)$ を任意に与えるとき，射 $f: Y \longrightarrow \Pi$ で $f_i = p_i \circ f$ となるものが唯一つ存在する．



双対的に，**双対直積（直和）** も定義される．集合の圏や，加群の圏などでは，これらは通常の直積や直和と一致する．



例 1.6　圏 $\mathscr{C}$ の対象 S を1つ固定する．このとき，$X \in \mathscr{C}$ と，射 $f: X \longrightarrow S$ の組を，**S 上の対象** とよぶ．S 上の対象の全体は，右図のような可換性を満たす $\mathscr{C}$ での射 $h: X \longrightarrow Y$ を射として，1つの圏をなす．この場合，$f: X \longrightarrow S$ を **構造射**，$h: X \longrightarrow Y$ を **S 射** とよび，この新しくできた圏を $\mathscr{C}/S$ で表す．この圏 $\mathscr{C}/S$ における S 上の対象の直積を **ファイバー積** とよび，$X \prod_S Y$ などと表す．双対的に，**ファイバー和** $X \coprod_S Y$ も定義できる．



§2.　関　手

F が圏 $\mathscr{C}$ から圏 $\mathscr{C}'$ への **共変関手** であるとは，$\mathscr{C}$ の対象 X に対し，$\mathscr{C}'$ の対象 $F(X)$ を対応させ，$\mathscr{C}$ での射 $f: X \longrightarrow Y$ に対し $\mathscr{C}'$ での射 $F(f): F(X) \longrightarrow F(Y)$ を対応させる写像で，次の2条件を満たすものをいう：

(F 1)　　$F(1_X) = 1_{F(X)}$,

(F 2)　　$F(g \circ f) = F(g) \circ F(f)$.

双対的に，$\mathscr{C}$ の対象 X に $\mathscr{C}'$ の対象 $F(X)$ を対応させ，$\mathscr{C}$ での射 $f: X \longrightarrow Y$ に対し，$\mathscr{C}'$ での射 $F(f): F(Y) \longrightarrow F(X)$ で，**(F 1)** と

(F 2)′　　$F(g \circ f) = F(f) \circ F(g)$

を満たすものとして，**反変関手**が定義される．反変関手 $F:\mathscr{C}\longrightarrow\mathscr{C}'$ は，$\mathscr{C}$ の双対圏 $\mathscr{C}^o$ から $\mathscr{C}'$ への共変関手と思える．多変数の関手も，圏の直積よりの関手として定義される．

共変(反変)関手 $F:\mathscr{C}\longrightarrow\mathscr{C}'$ は，任意の $X, Y\in\mathscr{C}$ について，$f\longmapsto F(f)$ なる対応により定まる

$$F:\quad \mathrm{Hom}_{\mathscr{C}}(X, Y)\longrightarrow \mathrm{Hom}_{\mathscr{C}'}(F(X), F(Y))$$

(反変のときは，$F(X)$ と $F(Y)$ をおき換える）が単射となるとき，**忠実**であるという．また，これが全射のとき，**充満**であるという．とくに，忠実な関手 $F:\mathscr{C}\longrightarrow\mathscr{C}'$ で，

$$X\neq Y \implies F(X)\neq F(Y)$$

を満たすものを**埋め込み**という．この場合には，$\mathscr{C}$ は $\mathscr{C}'$ の部分圏と同一視できる．

忠実かつ充満な共変関手 $F:\mathscr{C}\longrightarrow\mathscr{C}'$ が，任意の $X'\in\mathscr{C}'$ に対し，ある $X\in\mathscr{C}$ と，$\mathscr{C}'$ での同型射 $F(X)\cong X'$ が存在するとき，F を圏の**同値**であるという．この場合，圏 $\mathscr{C}$ と圏 $\mathscr{C}'$ とは同一視できる．同様にして，反変関手についても，($\mathscr{C}$ の双対圏 $\mathscr{C}^o$ より $\mathscr{C}'$ への圏の同値を与えるものとして，) **反同値** $F:\mathscr{C}\longrightarrow\mathscr{C}'$ が定義される．

例 2. 1 群 G を単に集合とみなし，群の準同型 $f: G\longrightarrow G'$ を単に集合の間の写像とみなすことにより，群の圏より集合の圏への関手が定義される．このように，圏における構造の一部を無視（忘却）することにより得られる関手を，**忘却関手**とよぶ．

例 2. 2 左 R-加群 M に，その双対加群 $M^*=\mathrm{Hom}_R(M, R)$ を対応させ，左 R-加群の準同型 $f: M\longrightarrow M'$ にその転置写像

$${}^t f:\quad (M')^*=\mathrm{Hom}_R(M', R)\ni\varphi \longmapsto \varphi\circ f\in \mathrm{Hom}_R(M, R)=M^*$$

を対応させると，左 R-加群のなす圏より，右 R-加群のなす圏への反変関手が得られる．

例 2. 3 $\mathscr{C}$ を圏とし，$X\in\mathscr{C}$ を固定する．このとき，$Y\in\mathscr{C}$ に対し集合 $\mathrm{Hom}_{\mathscr{C}}(X, Y)$ を対応させ，射 $f: Y\longrightarrow Y'$ に対し，$f_*:\mathrm{Hom}_{\mathscr{C}}(X, Y)\ni g\longmapsto f\circ g\in \mathrm{Hom}_{\mathscr{C}}(X, Y')$ を対応させることにより，$\mathscr{C}$ から集合のなす圏 (Sets) への共変関手 $h_X:\mathscr{C}\longrightarrow$

(Set) を得る．同様にして，$Y \in \mathscr{C}$ に対し集合 $\mathrm{Hom}_{\mathscr{C}}(Y, X)$ を対応させ，射 $f: Y \longrightarrow Y'$ に対し $f^*: \mathrm{Hom}_{\mathscr{C}}(Y', X) \ni g \longmapsto g \circ f \in \mathrm{Hom}_{\mathscr{C}}(Y, X)$ を対応させることにより，反変関手 $h^X: \mathscr{C} \longrightarrow$ (Sets) が得られる．

$\mathscr{C}, \mathscr{C}'$ を圏とするとき，共変関手 $\mathscr{C} \longrightarrow \mathscr{C}'$ の全体を，$\mathrm{Hom}(\mathscr{C}, \mathscr{C}')$ で表す．$F, G \in \mathrm{Hom}(\mathscr{C}, \mathscr{C}')$ のとき，F から G への **(関手間の) 射** または **自然変換** とは，すべての $X \in \mathscr{C}$ に $\mathscr{C}'$ での射 $\varphi(X): F(X) \longrightarrow G(X)$ を対応させる関数 φ で，$f: X \longrightarrow Y$ を $\mathscr{C}$ での射とするとき，右図が可換となるものをいう．反変関手に対しても射が，同様に定義される．

$$\begin{array}{ccc} F(X) & \xrightarrow{\varphi(X)} & G(X) \\ {\scriptstyle F(f)}\downarrow & \circlearrowleft & \downarrow{\scriptstyle G(f)} \\ F(Y) & \xrightarrow[\varphi(Y)]{} & G(Y) \end{array}$$

関手間の射 $\varphi: F \longrightarrow G$ で，任意の $X \in \mathscr{C}$ について $\varphi(X): F(X) \longrightarrow G(X)$ が同型となるとき，φ を **関手間の同型射** または **同型** といい $\varphi: F \xrightarrow{\sim} G$ と表す．

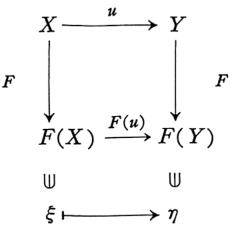
$\mathscr{C}$ を小さい圏，$\mathscr{C}'$ を圏とする．このとき $\mathrm{Ob}(\mathscr{C})$ は集合だから，共変関手 $F, G: \mathscr{C} \longrightarrow \mathscr{C}'$ の間の射 φ の全体は，埋め込み $\varphi \longmapsto \prod_{X \in \mathscr{C}} \varphi(X)$ により，$\prod_{X \in \mathscr{C}} \mathrm{Hom}(F(X), G(X))$ の部分集合となる．これを $\mathrm{Hom}(F, G)$ で表すと，共変関手の全体 $\mathrm{Hom}(\mathscr{C}, \mathscr{C}')$ は，自然変換を射として圏をなす．また反変関手 $H: \mathscr{C} \longrightarrow \mathscr{C}'$ は，双対圏 $\mathscr{C}^o$ から $\mathscr{C}'$ への共変関手であるから，$\mathscr{C}$ が小さい圏なら，反変関手 $H: \mathscr{C} \longrightarrow \mathscr{C}'$ の全体も圏 $\mathrm{Hom}(\mathscr{C}^o, \mathscr{C}')$ をなす．

$F: \mathscr{C} \longrightarrow \mathscr{C}'$，$F': \mathscr{C}' \longrightarrow \mathscr{C}$ を圏の間の共変関手とする．いま任意の $X \in \mathscr{C}$ と $X' \in \mathscr{C}'$ に対し，全単射 $\theta_{X,X'}: \mathrm{Hom}_{\mathscr{C}}(X, F'(X)) \longrightarrow \mathrm{Hom}_{\mathscr{C}'}(F(X), X')$ が対応づけられ，かつ $\mathscr{C}$ の射 $X \longrightarrow Y$ と $\mathscr{C}'$ の射 $X' \longrightarrow Y'$ より定まる下図が可換となるものとする．

$$\begin{array}{ccc} \mathrm{Hom}_{\mathscr{C}}(X, F'(X')) & \xrightarrow[\theta_{X,X'}]{} & \mathrm{Hom}_{\mathscr{C}'}(F(X), X') \\ \downarrow & \circlearrowleft & \downarrow \\ \mathrm{Hom}_{\mathscr{C}}(Y, F'(Y')) & \xrightarrow[\theta_{Y,Y'}]{} & \mathrm{Hom}_{\mathscr{C}'}(F(Y), Y') \end{array}$$

このとき，F を F' の **左随伴関手**，F' を F の **右随伴関手** という．これは，

$\mathscr{C} \times \mathscr{C}'$ から集合のなす圏への関手として，$\mathrm{Hom}_{\mathscr{C}'}(F(X), X')$ と $\mathrm{Hom}_{\mathscr{C}}(X, F'(X))$ が同型であることを意味する．



$F: \mathscr{C} \longrightarrow$ (Sets) を圏 $\mathscr{C}$ から集合のなす圏への共変関手とする．このとき，$X \in \mathscr{C}$ と $\xi \in F(X)$ で，任意の $Y \in \mathscr{C}$ と $\eta \in F(Y)$ に対し，$\mathscr{C}$ の射 $u: X \longrightarrow Y$ で $F(u)\xi = \eta$ となるものが一意的に存在するなら，組 (X, ξ) は関手 F を **表現する** といい，ξ を $F(X)$ の **標準元** であるという．F が反変関手のときも，u を $u: Y \longrightarrow X$ と修正することにより定義できる．

例 2.4 $\mathscr{C}$ を小さい圏とし，$F: \mathscr{C} \longrightarrow$ (Sets) を共変関手とする．そこで，$X \in \mathscr{C}$ に対し h_X を例 2.3 の通りとし，F と h_X を圏 $\mathrm{Hom}(\mathscr{C}, (\mathrm{Set}))$ の元と思う．h_X から F への関手間の射に対し集合 $F(X)$ の元を対応させる写像 $\Phi_X: \mathrm{Hom}(h_X, F) \longrightarrow F(X)$ を，$\Phi_X(\varphi) = \varphi(X)(1_X)$ で定義する．このとき Φ_X は全単射となり，その逆写像は $\xi \in F(X)$ に対し，$\varphi(Y)(u) = F(u)(\xi)$ $(Y \in \mathscr{C},\ u \in h_X(Y) = \mathrm{Hom}_{\mathscr{C}}(X, Y))$ とおくことで得られる．とくに $F = h_Y$ とおくと，標準的全単射 $\mathrm{Hom}(h_X, h_Y) \cong \mathrm{Hom}(Y, X)$ が得られる．したがって，$X \in \mathscr{C}$ に対し h_X を対応させ，$\mathscr{C}$ での射には上の標準的全単射で対応する関手間の射を対応させることにより，充満忠実な反変関手 $\mathscr{C} \longrightarrow \mathrm{Hom}(\mathscr{C}, (\mathrm{Set}))$ を得る．同様にして，h_X の代りに h^X をとると，充満忠実な共変関手 $\mathscr{C} \longrightarrow \mathrm{Hom}(\mathscr{C}^o, (\mathrm{Sets}))$ を得る．ここで $\mathscr{C}^o$ は $\mathscr{C}$ の双対圏とする．

例 2.5 A, B を環とし，L を (B, A)-両側加群，${}_A\mathscr{M}$, ${}_B\mathscr{M}$ を各々左 A-加群，左 B-加群のなす圏とする．関手 $F: {}_A\mathscr{M} \longrightarrow {}_B\mathscr{M}$ と $F': {}_B\mathscr{M} \longrightarrow {}_A\mathscr{M}$ を

$$F(X) = L \otimes_A X, \qquad F'(X') = \mathrm{Hom}_B(L, X')$$

で定義する．このとき標準的な同型（第Ⅳ章，問題 2.6 参照）

$$\mathrm{Hom}_B(L \otimes_A X, X') \simeq \mathrm{Hom}_A(X, \mathrm{Hom}_B(L, X'))$$

が成り立つから，F は F' の左随伴関手となり，F' は F の右随伴関手となる．

例 2.6 R を可換環とし，S をその乗法的閉集合とする．Y を任意の可換環とするとき，

$$F(Y) = \{h: R \longrightarrow Y \mid \text{環の準同型写像},\ h(S) \subset U(Y)\}$$

とし，準同型写像 $f: Y \longrightarrow Y'$ に対し，写像の合成により $F(f): F(Y) \ni h \longmapsto f \circ h \in F(Y')$ を定める．このとき，F は可換環のなす圏 (Rings) から集合のなす圏 (Sets) への共変関手を定める．この関手は，商環の普遍性（第III章，定理 3.2）により，商環 R_S と環の準同型 $i: R \longrightarrow R_S$ の組により表現される．テンソル積の普遍性なども同様に解釈できる．

§3. 加法圏とアーベル圏

圏 $\mathscr{C}$ において $\mathrm{Hom}_{\mathscr{C}}(X, Y)$ $(X, Y \in \mathscr{C})$ がアーベル群の構造をもち，次の 3 条件を満たすとき，$\mathscr{C}$ を **加法圏** とよぶ．

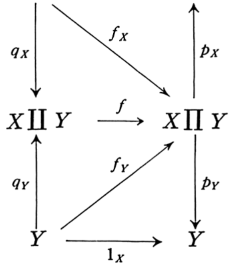
(AD 1) 射の合成が分配法則を満たす：

$$(f_1 + f_2) \circ g = f_1 \circ g + f_2 \circ g,$$
$$f \circ (g_1 + g_2) = f \circ g_1 + f \circ g_2$$

(AD 2) 零対象 $0 \in \mathscr{C}$ が存在する．

(AD 3) 任意の $X, Y \in \mathscr{C}$ に対し，その直積 $X \prod Y$ と直和 $X \coprod Y$ が存在する．

0 は零対象だから，任意の $X \in \mathscr{C}$ に対し，射 $0 \longrightarrow X$ と $X \longrightarrow 0$ が唯一つ存在する．よって，任意の $X, Y \in \mathscr{C}$ に対し，射 $X \longrightarrow 0 \longrightarrow Y$ の合成として $0: X \longrightarrow Y$ が作れる．この $0: X \longrightarrow Y$ は $0 + 0 = 0$ を満たすから，$\mathrm{Hom}_{\mathscr{C}}(X, Y)$ の単位元となる．



そこで，射 $1_X: X \longrightarrow X$ と射 $0: X \longrightarrow Y$ の組に直積の普遍性を使うと，射 $f_X: X \longrightarrow X \prod Y$ ができる．同様にして，射 $f_Y: Y \longrightarrow X \prod Y$ もできる．よって，直和の普遍性より，射 $f: X \coprod Y \longrightarrow X \prod Y$ で右図を可換にするものが唯一つ存在する．そこで $g = q_X \circ p_X + q_Y \circ p_Y: X \prod Y \longrightarrow X \coprod Y$ とおくと，f の定義より $f \circ g$

$=1_{X\amalg Y}$，$g\circ f=1_{X\amalg Y}$ となり，$f:X\amalg Y\longrightarrow X\prod Y$ は同型となる．したがって，加法圏では，2つの対象の直積と直和は同一視できる．

$\mathscr{C}$ が加法圏であり，さらに次の2条件 (**AB 1**), (**AB 2**) を満たすとき，**アーベル圏** であるという．

(**AB 1**)　任意の $\mathscr{C}$ の射 $f:X\longrightarrow Y$ は，核 $\mathrm{Ker}(f)$ と余核 $\mathrm{Coker}(f)$ をもつ．

$\mathscr{C}$ の射 $f:X\longrightarrow Y$ より，

$$\mathrm{Ker}(f)\longrightarrow X\xrightarrow{f}Y\longrightarrow\mathrm{Coker}(f)$$

を作る．そこで $\mathrm{Ker}(f)\longrightarrow X$ の余核を **余像** $\mathrm{Coim}(f)$，$Y\longrightarrow\mathrm{Coker}(f)$ の核を **像** $\mathrm{Im}(f)$ と表す．このとき定義より，$X\longrightarrow\mathrm{Coim}(f)\xrightarrow{\bar{f}}\mathrm{Im}(f)\longrightarrow Y$ の合成がもとの f となるような $\bar{f}:\mathrm{Coim}(f)\longrightarrow\mathrm{Im}(f)$ が唯一つ存在する．

(**AB 2**)　すべての $\mathscr{C}$ の射 $f:X\longrightarrow Y$ に対し，上のようにして作った $\bar{f}$：$\mathrm{Im}(f)\longrightarrow\mathrm{Coim}(f)$ が同型射である．

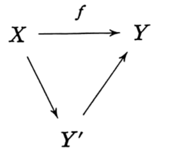
命題 3.1　$\mathscr{C}$ を加法圏とし，$f:X\longrightarrow Y$ を $\mathscr{C}$ の射とする．このとき f が単射となるための必要十分条件は，$0\longrightarrow X$ が $\mathrm{Ker}(f)$ となることであり，f が全射となるための必要十分条件は，$Y\longrightarrow 0$ が $\mathrm{Coker}(f)$ となることである．

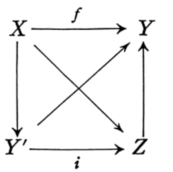
［**証明**］ f が単射なら $f\circ g=0=f\circ 0$ より $g=0$ を得る．よって $0\longrightarrow X$ が $\mathrm{Ker}(f)$ となる．逆に $0\longrightarrow X$ が $\mathrm{Ker}(f)$ を与えるとする．このとき $f\circ g_1=f\circ g_2$ なら $f\circ(g_1-g_2)=0$ となり，$g_1=g_2$ となる．よって f は単射となる．後半は前半の双対化（矢印を逆にする）で得られる．　(証明終)

命題 3.2　アーベル圏において全単射は同型となる．

［**証明**］ $\mathscr{C}$ をアーベル圏とし，$f:X\longrightarrow Y$ が全単射だとする．このとき，命題 3.1 より $0\longrightarrow X$ が $\mathrm{Ker}(f)$ をなし，$Y\longrightarrow 0$ が $\mathrm{Coker}(f)$ をなす．したがって，$\mathrm{Coim}(f)=1_X:X\longrightarrow X$，$\mathrm{Im}(f)=1_Y:Y\longrightarrow Y$ となる．よって (**AB 2**) より，$\bar{f}=f:X\longrightarrow Y$ は同型射となる．　(証明終)

$\mathscr{C}$ をアーベル圏とし，$f: X \longrightarrow Y$ を $\mathscr{C}$ の射とする．このとき $\mathrm{Im}(f): Y' \longrightarrow Y$ を f の像とすると，右図のような可換図式ができる．しかも $Z \longrightarrow Y$ もこの可換図式を満たすなら，右図を可換にする $i: Y' \longrightarrow Z$ が存在する．逆に $Y' \longrightarrow Y$ がこの性質をもつなら，これが像となることもわかる．Coim(f) についても，同様の特徴づけが得られる．





$\mathscr{C}$ の射 $f: X \longrightarrow Y$ が全射となるための必要十分条件は，$Y \longrightarrow 0$ が余核となることであった．したがって，f が全射なら $1_Y: Y \longrightarrow Y$ が f の像となる．逆に $1_X: Y \longrightarrow Y$ が f の像なら，$Y \longrightarrow 0$ が f の余核となる．よって f が全射となるための必要十分条件は，$1_X: Y \longrightarrow Y$ が f の像となることである．

$\mathscr{C}$ をアーベル圏とし，

$$\cdots \longrightarrow X_{n+1} \xrightarrow{f_{n+1}} X_n \xrightarrow{f_n} X_{n-1} \longrightarrow \cdots$$

を $\mathscr{C}$ の射の列とする．このとき，すべての n について $\mathrm{Im}(f_{n+1}) = \mathrm{Ker}(f_n)$ が成り立つとき，この射の列は**完全**であるという．アーベル圏からアーベル圏への関手で，完全系列を完全系列にうつすものを**完全関手**とよぶ．

例 3. 3　R を環とし，${}_R\mathscr{M}$ を左 R-加群のなす圏とすると，${}_R\mathscr{M}$ は核と余核をもちアーベル圏となる．一般に Ob$(\mathscr{C})$ が集合であるようなアーベル圏 $\mathscr{C}$ は，ある環 R 上の左 R-加群の圏 ${}_R\mathscr{M}$ に共変完全関手により埋め込めることが知られている（B. Mitchell の充満埋め込み定理，Amer. J. Math. 86(1964)）．

問 題 略 解

第 I 章

問 題 1. 1 A と $\mathrm{Im}(f)$ の元の個数を比較せよ.

問 題 4. 3 n 個より数の少ない積では括弧のつけ方によらないものとすれば, $(a_1\cdot a_2\cdots a_r)(a_{r+1}\cdot a_{r+2}\cdots a_n)=(a_1\cdot a_2\cdots a_{n-1})\cdot a_n$ がすべての r について成り立つことを示せばよい.

問 題 5. 1 $a\in G$ を任意にとり, $ax=a$ となる元 x を 1 とおく. また $ay=1$ となる元 y を a^{-1} とおく.

問 題 5. 2 $x=y \Longleftrightarrow x^{-1}=y^{-1} \Longleftrightarrow ax=ay \Longleftrightarrow xa=ya$ が成り立つから単射であり, x が与えられたとき, $x^{-1}=z$, $au=x$, $va=x$ は $z=x^{-1}$, $u=a^{-1}x$, $v=xa^{-1}$ によって満たされるから全射である.

問 題 9. 3 α が n 次多項式 $f(x)\in R[x]$ の根なら, 系 9.2 より $f(x)=(x-\alpha)f_1(x)$ となる $f_1(x)\in R[x]$ があり, $\deg f_1(x)=\deg f(x)-1$ となる.

問 題 9. 4

$$f(x_1,x_2,\cdots,x_n)=\sum a_m(x_1,x_2,\cdots,x_{n-1}){x_n}^m,$$
$$g(x_1,x_2,\cdots,x_n)=\sum b_m(x_1,x_2,\cdots,x_{n-1}){x_n}^m$$

($a_m(x_1,x_2,\cdots,x_{n-1})$, $b_m(x_1,x_2,\cdots,x_{n-1})\in R[x_1,x_2,\cdots,x_{n-1}]$) とおく. 仮定より $f\neq g$ だから, ある m に対して $a_m\neq b_m$ となる. n に関する帰納法で, $\alpha_1,\alpha_2,\cdots,\alpha_{n-1}\in R$ を $a_m(\alpha_1,\alpha_2,\cdots,\alpha_{n-1})\neq b_m(\alpha_1,\alpha_2,\cdots,\alpha_{n-1})$ なるようにとり, $f^*(x_n)=f(\alpha_1,\alpha_2,\cdots,\alpha_{n-1},x_n)$ と $g^*(x_n)=g(\alpha_1,\alpha_2,\cdots,\alpha_{n-1},x_n)$ を考える. $\alpha_1,\alpha_2,\cdots,\alpha_{n-1}$ のとり方より $f^*(x_n)\neq g^*(x_n)$ であるから, $\alpha_n\in R$ で $f^*(\alpha_n)=g^*(\alpha_n)$ となるものは有限個である. R は無限個の元をもつから, それ以外の α_n をとればよい.

問 題 10. 1 $\sum_j a_{ij}(\sum_k b_{jk}c_{kl})=\sum_k(\sum_j a_{ij}b_{jk})c_{kl}$ が成り立つ.

第 II 章

問題 1. 4 （1） H, K について (SG 1), (SG 2) が成り立つことから，$H \cap K$ についても (SG 1), (SG 2) が成り立つことをみればよい．

（2） $H \cdot K$ が部分群なら $H, K \subset H \cdot K$ より $K \cdot H \subset H \cdot K$ となる．これを $a \longmapsto a^{-1}$ なる写像でうつすと，$H \cdot K = (K \cdot H)^{-1} \subset (H \cdot K)^{-1} = K \cdot H$ となり $K \cdot H = H \cdot K$ が成り立つ．逆に $H \cdot K = K \cdot H$ なら，$(H \cdot K)(H \cdot K) = H \cdot (K \cdot H) \cdot K = H \cdot (H \cdot K) \cdot K \subset H \cdot K$, $(H \cdot K)^{-1} = K^{-1} \cdot H^{-1} = K \cdot H \subset H \cdot K$ より $H \cdot K$ は部分群となる．

問題 1. 9 $a \sim b \Longleftrightarrow a = hbk$ $(\exists h \in H, \exists k \in K)$ である．$a = 1 \cdot b \cdot 1$, $b = h^{-1}ak^{-1}$ より反射律，対称律が成り立つ．推移律の証明も容易である．

問題 2. 1 （1） $aN_i a^{-1} = N_i$ なら $a(N_1 \cap N_2)a^{-1} = (aN_1a^{-1}) \cap (aN_2a^{-1}) = N_1 \cap N_2$, $a(N_1 \cdot N_2)a^{-1} = (aN_1a^{-1})(aN_2a^{-1}) = N_1 \cdot N_2$.

（2） $aNa^{-1} = N$ より，$a \in H$ なら $a(H \cap N)a^{-1} = H \cap (aNa^{-1}) = H \cap N$, また $aN = Na$ $(a \in H)$ より $H \cdot N = N \cdot H$ となる（問 1. 4 参照）．

問題 2. 8 $a \in G_3$ が $f_3(a) = 1$ を満たすとする．可換性より $f_4(h_3(a)) = h_3'(f_3(a)) = 1$ だから，$h_3(a) = 1$ となる．よって $b \in G_2$ があり，$a = h_2(b)$ となる．このとき $h_2'(f_2(b)) = f_3(h_2(b)) = f_3(a) = 1$ だから，$c' \in G_1'$ があり $f_2(b) = h_1'(c')$ となる．$c' = f_1(c)$ $(c \in G_1)$ と書くと，$f_2(h_1(c)) = h_1'(f_1(c)) = h_1'(c') = f_2(b)$ だから，$b = h_1(c)$ となる．よって $a = h_2(b) = h_2(h_1(c)) = 1$ となり，f_3 は単射となる．全射の証明も同様である．f_1 は全射，f_5 は単射であることのみを使う．

問題 3. 4 必要性は明らかである．十分性を示すため，σ と τ が共に型 $1^{m_1}2^{m_2}\cdots n^{m_n}$ であるとする．$\sigma = \prod_{1 \leq i \leq n} \prod_{1 \leq j \leq m_i} (a^{(ij)}{}_1,\ a^{(ij)}{}_2,\ \cdots, a^{(ij)}{}_i)$, $\tau = \prod_{1 \leq i \leq n} \prod_{1 \leq j \leq m_i} (b^{(ij)}{}_1,\ b^{(ij)}{}_2, \cdots,\ b^{(ij)}{}_i)$ を定理 3. 3 の分解とすると，σ と τ は $a^{(ij)}{}_k \longmapsto b^{(ij)}{}_k$ $(\forall i, \forall j, \forall k)$ とする置換 $\rho \in S_n$ により共役となる．

問題 3. 6 n に関する帰納法で，$n-1$ 次対称群 S_{n-1} は $\{(1\ 2), (2\ 3), \cdots, (n-2\ \ n-1)\}$ により生成されると仮定する．$\sigma \in S_n$ が $\sigma(n) = m$ を満たすとすると，$\tau = (n-1\ \ n)(n-2\ \ n-1)\cdots\cdots(m\ \ m+1)\sigma = (n, n-1, \cdots, m)\sigma$ は $\tau(n) = n$ を満たす．よって仮定より，τ は $\{(1\ 2),\ (2\ 3), \cdots,\ (n-2\ \ n-1)\}$ の積として表される．

問題5.3 nに関する帰納法で，定理5.1と定理5.2に帰着させる．

問題6.4 定理6.2の記号で，$t \geqq 2 \Longleftrightarrow \sharp\{g \in G \mid e_1 g = 0\} \geqq e_1{}^2$が成り立つ．これより十分性がでる．必要性は例2.6より明らかである．

問題8.20 (1) 中心列を部分群に制限しても，剰余群に移しても中心列となる．

(2) Gの中心列を $C : G = G_0 \supset G_1 \supset \cdots \supset G_l = \{1\}$，$G'$の中心列を $C' : G' = G_0{}' \supset G_1{}' \supset \cdots \supset G_m = \{1\}$ とすると，$C'' : G \times G' = G_0 \times G_0{}' \supset G_1 \times G_0{}' \supset \cdots \supset G_l \times G_0{}' \simeq G' \supset G_l \times G_1{}' \supset \cdots \supset G_l \times G_m{}' = \{1\}$が$G \times G'$の中心列となる．

第III章

問題1.3 $\mathfrak{a}\cdot\mathfrak{b} \subset \mathfrak{a} \cap \mathfrak{b}$は明らかである．$\mathfrak{a} + \mathfrak{b} = R$だから，$a + b = 1$ $(a \in \mathfrak{a},\ b \in \mathfrak{b})$とし，$c \in \mathfrak{a} \cap \mathfrak{b}$とする．このとき $c = ca + cb = ac + cb \in \mathfrak{a}\cdot\mathfrak{b}$ となる．

問題1.6 $S \cap \mathfrak{a}$がSの両側イデアルであることは明らかである．群の同型定理より，加法群として$S/S \cap \mathfrak{a} \simeq (S + \mathfrak{a})/\mathfrak{a}$が成り立つが，$a \pmod{S \cap \mathfrak{a}} \longmapsto a + \mathfrak{a} \pmod{\mathfrak{a}}$ なる対応は積を保ち，環の同型となる．

問題2.4 $\mathscr{B} = \{\mathfrak{b} \mid R \supsetneqq \mathfrak{b} \supseteqq \mathfrak{a},\ \text{左イデアル}\}$ とおき，定理2.2と同様の議論を行えばよい．

問題2.5 $\mathfrak{a} \not\subset \mathfrak{p}$，$\mathfrak{b} \not\subset \mathfrak{p}$とすると，$a \in \mathfrak{a}$と$b \in \mathfrak{b}$で，$a, b \notin \mathfrak{p}$となるものが存在する．このとき$\mathfrak{p}$は素イデアルだから，$ab \notin \mathfrak{p}$となるが，他方$ab \in \mathfrak{a}\cdot\mathfrak{b} \subset \mathfrak{p}$となり矛盾である．

問題3.7 商体は $a_{-m_0}x^{-m_0} + a_{-m_0+1}x^{-m_0+1} + \cdots + a_0 + a_1x^1 + a_2x^2 + \cdots$ $(a_{-m_0}, a_{-m_0+1}, \cdots, a_0, a_1 \cdots \in R)$ なるxのある負のべきから始まり，xの正のべきすべてを含むxのべき級数の全体である．例3.6を参照せよ．

問題3.8 $K[[x_1, x_2, \cdots, x_n]] \ni f(x_1, x_2, \cdots, x_n) \longmapsto f(0, 0, \cdots, 0) \in K$ の核を$\mathfrak{m}$とする．$f(x_1, x_2, \cdots, x_n) \notin \mathfrak{m}$なら$f(x_1, x_2, \cdots, x_n)$が$K[[x_1, x_2, \cdots, x_n]]$の単数となることを，例3.6と同様にして示す．

問題4.3 省略．

問題4.7 図より$(\beta/\alpha) - q = (c - m) + (d - n)\sqrt{-1}$において，$|c - m|$，$|d - m| \leqq 1/\sqrt{2}$である．しかも$c - m$，$d - n \in \boldsymbol{Q}$となるから，等号は成り立たない．

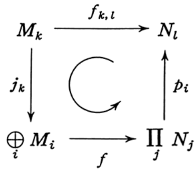
よって　$\varphi(r/\alpha)=\varphi((\beta/\alpha)-q)=(c-m)^2+(d-m)^2<1$　である．後は容易である．

問題 5.3　ヒントの $\mathfrak{a}_m$ を使い，定理 5.1 の証明と同様の議論を行う．

問題 5.4　i は環準同型だから，$i^{-1}(\mathfrak{a})$ は R のイデアルである．$i(i^{-1}(\mathfrak{a}))\subset\mathfrak{a}$ は明らかである．$i(a/s)\in\mathfrak{a}$ とする．このとき $i(a)=i(a/s)\cdot i(s)\in\mathfrak{a}$ だから，$a\in i^{-1}(\mathfrak{a})$ となる．よって $i(a/s)=i(a)i(s)^{-1}\in i(i^{-1}(\mathfrak{a}))R_S$ となり，$i(i^{-1}(\mathfrak{a}))R_S=\mathfrak{a}$ となる．R がネター環なら $i^{-1}(\mathfrak{a})$ は有限生成なイデアルだから，$\mathfrak{a}=i(i^{-1}(\mathfrak{a}))R_S$ も有限生成となる．

第 IV 章

問題 1.2　$f\in\mathrm{Hom}_R(\bigoplus_i M_i,\ \prod_j N_j)$ に対し，右の図を可換にするような $f_{k,l}: M_k\longrightarrow N_l$ を対応させ，$\mathrm{Hom}_R(\bigoplus M_i,\ \prod N_j)\longrightarrow\prod\mathrm{Hom}_R(M_iN_j)$ を作る．これは直積と直和の普遍性より全単射となる．



問題 1.5　$M=\bigoplus_{i\in I}M_i,\ M_i\simeq R$ とする．そこで M の元 $m=\sum_i m_i$ が，R の零因子でない元 $r\neq 0$ に対し $r\cdot m=\sum_i r\cdot m_i=0$ となったとする．このとき $r\cdot m_i=0\ (\forall i\in I)$ となり，r は零因子でないから $m_i=0$ となる．

問題 2.6　$n\in N$ を固定すると，$L\times M\ni(l,m)\longmapsto l\otimes(m\otimes n)\in L\otimes_R(M\otimes_S N)$ は準双 1 次写像であり，$f_n: L\otimes_R M\longrightarrow L\otimes_R(M\otimes_S N)$ なる準同型で $f_n(l,m)=l\otimes(m\otimes n)$ なるものに拡張される．ところが $(L\otimes_R M)\times N\ni(x,n)\longmapsto f_n(x)\in L\otimes_R(M\otimes_S N)$　は準双 1 次写像だから，$f: (L\otimes_R M)\otimes_S N\longrightarrow L\otimes_R(M\otimes_S N)$ で　$f((l\otimes m)\otimes n)=l\otimes(m\otimes n)$　なるものに拡張される．対称性より，f の逆写像 $g: L\otimes_R(M\otimes_S N)\longrightarrow(L\otimes_R M)\otimes_S N,\ g(l\otimes(m\otimes n))=(l\otimes m)\otimes n$　も作られる．後半も大体同様にして証明できる．

問題 2.7　$(\bigoplus_i M_i)\times(\bigoplus_j N_j)\ni(\sum_i m_i,\ \sum_j n_j)\longmapsto\sum_{ij}m_i\otimes n_j\in\bigoplus_{ij}M_i\otimes_R N_j$ は準双 1 次写像だから，$f: (\bigoplus_i M_i)\otimes_R(\bigoplus_j N_j)\longrightarrow\bigoplus_{ij}M_i\otimes_R N_j$ なる準同型に拡張される．他方，$m_k\in M_k$ と $n_l\in N_l$ に対し，k 成分のみ m_k で他は 0 となる $\bigoplus_i M_i$

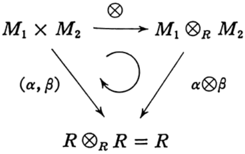
の元を $\tilde{m}_k$, l 成分のみ n_l で他は 0 となる $\oplus_j N_j$ の元を $\tilde{n}_l$ とする. $M_k \times N_l \ni (m_k, n_l) \longmapsto \tilde{m}_k \otimes \tilde{n}_l \in (\oplus_i M_i) \otimes_R (\oplus_j N_j)$ は準双1次写像で, $M_k \otimes N_l \longrightarrow (\oplus_i M_i) \otimes_R (\oplus_j N_j)$ なる準同型 $g_{k,l}$ に拡張される. k, l についての和をとると $g = \oplus_{ij} g_{i,j} : \oplus_{ij} M_i \otimes_R N_j \longrightarrow (\oplus_i M_i) \otimes_R (\oplus_j N_j)$ ができるが, これが f の逆写像を与える.

問 題 2. 9 第Ⅲ章, 問 5.4 と大体同様にして証明できる.

問 題 2. 13 $S(M)$ は定義より可換な多元環となる. そこで $\{u_1, u_2, \cdots, u_n\}$ を M の基底とし, $u_i \otimes u_i \otimes \cdots \otimes u_i$ (m_i 個のテンソル積) を $(u_i)^{m_i}$ で表すと, $S(M)$ の元は, $\sum_{m_1, m_2, \cdots, m_n \geq 0} a_{m_1 m_2 \cdots m_n} (u_1)^{m_1} (u_2)^{m_2} \cdots (u_n)^{m_n}$ $(a_{m_1 m_2 \cdots m_n} \in R)$ の形に一意的に表される.

問 題 2. 14 $a_i \in A_{p_i}$, $b_i \in B_{q_i}$ のとき, $\{(a_1 \otimes b_1)(a_2 \otimes b_2)\}(a_3 \otimes b_3) = (-1)^{q_1 p_2} (a_1 a_2 \otimes b_1 b_2)(a_3 \otimes b_3) = (-1)^{q_1 p_2 + (q_1 + q_2) p_3} a_1 a_2 a_3 \otimes b_1 b_2 b_3 = (-1)^{q_2 p_3} (a_1 \otimes b_1)(a_2 a_3 \otimes b_2 b_3) = (a_1 \otimes b_1)\{(a_2 \otimes b_2)(a_3 \otimes b_3)\}$ だから, この積は結合法則を満たし, $A \otimes_R B$ は多元環となる. 後半は, $M_1 \oplus M_2 \ni (m_1, m_2) \longmapsto m_1 \otimes 1 + 1 \otimes m_1 \in \wedge(M_1) \otimes \wedge(M_2)$ なる写像を, $T(M_1 \oplus M_2) \longrightarrow \wedge(M_1) \otimes \wedge(M_2)$ なる多元環の準同型に拡張し, それが $f : \wedge(M_1 \oplus M_2) \longrightarrow \wedge(M_1) \otimes \wedge(M_2)$ なる準同型をひきおこすことをいう. これが同型なことは, $M_i \hookrightarrow M_1 \oplus M_2$ よりひきおこされる $g : \wedge(M_1) \otimes \wedge(M_2) \longrightarrow \wedge(M_1 \oplus M_2)$, $g((a_1 \wedge \cdots \wedge a_p) \otimes (b_1 \wedge \cdots \wedge b_q)) = (a_1 \wedge \cdots \wedge a_p) \wedge (b_1 \wedge \cdots \wedge b_q)$ が逆写像を与えることからわかる.

問 題 3. 9 $n = 2$ としてよい. M_i $(i = 1, 2)$ を R-自由加群 F_i の直和因子とすると, $M_1 \otimes_R M_2$ は R-自由加群 $F_1 \otimes_R F_2$ の直和因子となり, (有限生成) 射影加群となる.



$M_i^* = \mathrm{Hom}_R(M_i, R)$, $(M_1 \otimes_R M_2)^* = \mathrm{Hom}_R(M_1 \otimes_R M_2, R)$ であるから, 命題 2.2 より, $f_M : M_1^* \otimes_R M_2^* \longrightarrow (M_1 \otimes_R M_2)^*$ なる準同型が作られる. $R^* = R$ であるから $f_F : F_1^* \otimes_R F_2^* \longrightarrow (F_1 \otimes_R F_2)^*$ は同型であり, これを直和成分に制限した f_M も同型である.

問 題 4. 9 完全性の定義を一つずつチェックすればよいが, これが 2 重複体をなすことを示し, 系 4.5 を使ってもよい.

問 題 4. 10 M, M'' の射影的分解を $P = \{P_n, \partial_n\}$, $P'' = \{P_n'', \partial_n''\}$ とおくと, $P_n' =$

$P_n \oplus P_n''$ は射影的で，直和分解に対応した短完全列 $0 \longrightarrow P_n \xrightarrow{f_n} P_n' \xrightarrow{g_n} P_n'' \longrightarrow 0$ が存在する．そこで $\partial_n' : P_n' \longrightarrow P'_{n-1}$ を条件を満たすよう帰納的に作ってゆく．$n-1$ までできたとし，$P_n' = P_n \oplus P_n''$ だから，$P_n \subset P_n \oplus P_n'' = P_n'$ 上では $\partial_n'|_{P_n} = f_{n-1} \circ \partial_n$ とおく．他方 $P_n'' \subset P_n \oplus P_n'' = P_n'$ 上では，P_n'' が射影的なことを使い，$g_{n-1} \circ \partial_n'|_{P_n''} = \partial_n''$ を満たすようにとる．このとき，n 番目の縦の列は完全で，n 番目より右の図式は可換となる．$P' = P \oplus P''$ が $\partial_n' = \partial_n'|_{P_n} \oplus \partial_n''|_{P_n''}$ に関して完全となることは，P, P'' の完全性より容易にでる．

$$
\begin{array}{ccccccc}
0 & & 0 & & 0 & & \\
\downarrow & & \downarrow & & \downarrow & & \\
P_n & \longrightarrow & P_{n-1} & \longrightarrow & P_{n-2} & \rightarrow & \cdots \\
\downarrow & & \downarrow & & \downarrow & & \\
P_n' & \longrightarrow & P'_{n-1} & \longrightarrow & P'_{n-2} & \rightarrow & \cdots \\
\downarrow & & \downarrow & & \downarrow & & \\
P_n'' & \longrightarrow & P''_{n-1} & \longrightarrow & P''_{n-2} & \rightarrow & \cdots \\
\downarrow & & \downarrow & & \downarrow & & \\
0 & & 0 & & 0 & &
\end{array}
$$

問題 5. 7　$M \simeq R/(e_1) \oplus \cdots \oplus R/(e_r) \oplus R \oplus \cdots \oplus R$ を定理 5. 2 の表示とする．自由加群は射影的で，射影的なら自由加群の直和因子だからねじれがない．ところが，いまの場合ねじれがないと $r=0$ となり，$M \simeq R^s$ となる．

問題 5. 12　次のように基本の変形を行う．

$$
\begin{pmatrix} 10 & 4 & 6 \\ 18 & 12 & 30 \end{pmatrix}
\xrightarrow[\text{1 列から 2 列の 2 倍を引く}]{}
\begin{pmatrix} 2 & 4 & 6 \\ -6 & 12 & 30 \end{pmatrix}
\xrightarrow[\text{3 列から 1 列の 3 倍を引く}]{\text{2 列から 1 列の 2 倍を引く}}
$$

$$
\begin{pmatrix} 2 & 0 & 0 \\ -6 & 24 & 48 \end{pmatrix}
\xrightarrow[\text{2 行に 1 行の 3 倍を加える}]{}
\begin{pmatrix} 2 & 0 & 0 \\ 0 & 24 & 48 \end{pmatrix}
\xrightarrow[\text{3 列から 2 列の 2 倍を引く}]{}
$$

$$
\begin{pmatrix} 2 & 0 & 0 \\ 0 & 24 & 0 \end{pmatrix} \quad \text{(標準形)}
$$

問題 5. 13　(1) $\Longleftrightarrow$ (2) は明らかである．(2) $\Longrightarrow$ (3) は相異なる λ_i について $x-\lambda_i$ の積を $f(x)$ とおき $f(A)$ を計算すればよい．(3) $\Longrightarrow$ (1) は，$f(x)=0$ の根を λ とするとき，λ が $f(x)$ の重根 $\Longleftrightarrow$ $f'(\lambda)=0$ なることを使えば，本文中の $f(A)$ の計算より明らかである．

問題 5. 14　A のジョルダンの標準形において，同じ固有値は続いて現れるようにし，それを左下図とする．このとき，この行列と可換な行列は，右下図のようになる：

$$
QAQ^{-1} = \begin{pmatrix} A_1 & & 0 \\ & \ddots & \\ 0 & & A_s \end{pmatrix}, \qquad A_i = \begin{pmatrix} \lambda_i & & 0 \\ & \ddots & \\ 0 & & \lambda_i \end{pmatrix}, \qquad QBQ^{-1} = \begin{pmatrix} B_1 & & 0 \\ & \ddots & \\ 0 & & B_s \end{pmatrix}
$$

つまり，QAQ^{-1} が対角行列で，同じ固有値は続いて現れるものとするとき，QAQ^{-1} を

固有値によりブロックに分けると，それと可換な行列も同じ型のブロックに分かれる．そこで QBQ^{-1} の各小ブロックに対し，再びジョルダンの標準形を作ればよい．

問題 5. 15 ジョルダンの標準形を PXP^{-1} とし，その対角部を D とする． $A = P^{-1}DP$, $B = X - P^{-1}DP$ とおくと，A は半単純，B はべき零で，$AB = BA$ となる．A, B がこの組に限ることは，問題 5.14 の議論より，A, B が同時にジョルダンの標準形とできることからわかる．

問題 5. 16 $\exp(z) = \sum_m z^m/m!$ は任意の $z \in \boldsymbol{C}$ に対し収束する．そこで A のジョルダンの標準形を PAP^{-1} とし，$P(\sum_m A^m/m!)P^{-1} = \sum_m (PAP^{-1})^m/m!$ が収束することを見ればよい．

問題 6. 15 D を斜体，$R = M_n(D)$ とする．このとき，R の極小左イデアルを $\mathfrak{a}$ とすると，定理 6.12 の証明より，$R \simeq n\mathfrak{a}$, $D \simeq \mathrm{End}_R(\mathfrak{a})$ となる．R のすべての極小左イデアルは同型であるから，これで $\Longrightarrow$ がでる．$\Longleftarrow$ は明らかである．

問題 6. 16 $\mathrm{Ann}(M)$ は R の両側イデアルで，R の M への作用は，$\bar{R} = R/\mathrm{Ann}(M)$ の M への作用を持ち上げたものとなる．$R = R_1 \oplus R_2 \oplus \cdots \oplus R_s$ を単純環の直和への分解とする．M は既約な左 $\bar{R}$-加群で，$\bar{R}$ の M への作用は忠実だから，$\bar{R}$ は唯一つしか直和成分をもたず，ある R_i と同型となる．よって M は既約な R_i-加群となるから，ある R_i の極小左イデアルと同型となる．

第 V 章

問題 2. 12 (1) と (2) の同値性は，定理 1.4 より得られる．(3) から (2) がでるのは明らかだが，定理 2.8, (2) より，$\sigma_0 : K(\alpha) \xrightarrow{\sim} K(\beta)$ なる K-同型は $\bar{K}/K$ の自己同型に拡張できる．

問題 3. 4 問題 2.12 の (3) と系 3.3 より明らかである．

問題 4. 10 ヒントより，L/K が単拡大なら $[L:K] = p$ となる．これは，$[L:K] = p^2$ に矛盾する．

問題 6. 7 $\mathrm{Gal}(\boldsymbol{Q}(\zeta)/\boldsymbol{Q}) \simeq U(\boldsymbol{Z}/7\boldsymbol{Z}) \simeq \boldsymbol{Z}/6\boldsymbol{Z} \simeq \boldsymbol{Z}/2\boldsymbol{Z} \times \boldsymbol{Z}/3\boldsymbol{Z}$ だから，$\boldsymbol{Q}(\zeta)/\boldsymbol{Q}$ の自明でない中間体は，$[K_3 : \boldsymbol{Q}] = 3$, $[K_2 : \boldsymbol{Q}] = 2$ の 2 つである．$K_3 = \boldsymbol{Q}(\zeta + \zeta^{-1}) = \boldsymbol{Q}(\zeta) \cap \boldsymbol{R}$, $K_2 = \boldsymbol{Q}(\zeta + \zeta^2 + \zeta^4) = \boldsymbol{Q}(\sqrt{-7})$ となる．$\zeta + \zeta^2 + \zeta^4 = (-1 +$

$\sqrt{-7})/2$ に注意する．

問題 6.8 $\bar{\boldsymbol{F}}_p$ の元は $\boldsymbol{F}_p$ 上代数的だから，$\bigcup \boldsymbol{F}_{p^n}$ に入る．ところが，$\bigcup \boldsymbol{F}_{p^n}$ は $\boldsymbol{F}_p$ の代数拡大だから，$\bar{\boldsymbol{F}}_p$ と一致する．

問題 7.8 系 7.7 の証明と注の $H^1(G,L)=0$ をあわせる．

問題 9.2 仮定より，$x_1, x_2, \cdots, x_m \in M$ で，K 上代数的に独立で，M は $K(x_1, x_2, \cdots, x_m)$ 上代数的なものが存在する．また $y_1, y_2, \cdots, y_n \in L$ で，M 上代数的に独立で，L は $M(y_1, y_2, \cdots, y_n)$ 上代数的なものが存在する．明らかに，$x_1, x_2, \cdots, x_m$ と $y_1, y_2, \cdots, y_n$ は K 上代数的に独立である．しかも，$L/M(y_1, y_2, \cdots, y_n)$，$M/K(x_1, x_2, \cdots, x_m)$ は代数的だから，L は $K(x_1, x_2, \cdots, x_m,\ y_1, y_2, \cdots, y_n)$ 上代数的である．よって

$$\text{trans.deg}_K L = m+n = \text{trans.deg}_K M + \text{trans.deg}_M K.$$

問題 9.3 $y=(ax+b)/(cx+d)$ $(a,b,c,d\in K,\ ad-bc\neq 0)$ なら，$x=(dy-b)/(-cy+a)$ と書ける．よって $x\longmapsto(ax+b)/(cx+d)$ は $K(x)/K$ の自己同型である．逆に $\sigma\in\mathrm{Aut}(L/K)$ とすると，$K(x)=K(\sigma(x))\ni\sigma(x)$ である．そこで $y=\sigma(x)=g(x)/h(x)$ $(g(x),\ h(x)\in K[x])$ とおき，この式の分母を払い整理すると，$f(x,y)=0$ $(f(x,y)\in K[x,y])$ の形の方程式を得る．ここで $f(x,y)=h(x)y-g(x)$ は y の 1 次式である．そこで多項式環 $K[x,y]$ で $f(x,y)$ を既約因子に分解すると，$f(x,y)=f_1(x)f_2(x)\cdots f_t(x)F(x,y)$ $(f_i(x)\in K[x]$，$F(x,y)\in K[x,y]$ は y の 1 次式$)$ の形となる．ここで x は K 上超越的だから，$f_i(x)\neq 0$ であり，よって $F(x,y)=0$ となる．ところが $[L:K(y)]=[L:K(x)]=1$ だから，$F(x,y)$ は x についても 1 次式である．よって

$$F(x,y)=cxy-ax+dy-b \qquad (a,b,c,d\in K)$$

とおくと，$y=(ax+b)/(cx+d)$ となる．$ad-bc=0$ なら，$y\in K$ となり矛盾する．

章末問題略解

第 I 章

1. 正六面体の回転で4つの対角線を固定するものは単位元となることと，4つの対角線を任意に置換する正六面体の回転が存在することをいえばよい．

2. $f(x)=\sum_{1\leq i\leq n+1}\beta_i\dfrac{(x-\alpha_1)\cdots(x-\alpha_{i-1})(x-\alpha_{i+1})\cdots(x-\alpha_{n+1})}{(\alpha_i-\alpha_1)\cdots(\alpha_i-\alpha_{i-1})(\alpha_i-\alpha_{i+1})\cdots(\alpha_i-\alpha_{n+1})}$

3. （1）は計算のみ，略．（2）は（1）の式を $m=1,2,\cdots,n$ まで連立させた式を解き，$\sigma_1,\sigma_2,\cdots,\sigma_n\in \boldsymbol{Q}$ がわかる．

4. $a_{ij}=0$ $(n_1<i,\ j\leqq n_1)$ より，$\det(A)$ の定義式で，σ が $\{1,2,\cdots,n_1\}$ を $\{1,2,\cdots,n_1\}$ にうつさないときは0となる．そこで $\sigma_1=\sigma|_{\{1,2,\cdots,n_1\}}$, $\sigma_4=\sigma|_{\{n_1+1,\cdots,n_1+n_2\}}$ とおくと，$\mathrm{sgn}(\sigma)=\mathrm{sgn}(\sigma_1)\,\mathrm{sgn}(\sigma_4)$ で，

$$\det(A)=\sum_{\sigma_1}\mathrm{sgn}(\sigma_1)\,a_{1\,\sigma_1(1)}\cdots a_{n_1\sigma_1(n_1)}\sum_{\sigma_4}\mathrm{sgn}(\sigma_4)\,a_{(n_1+1)\,\sigma_4(n_1+1)}\cdots a_{(n_1+n_2)\,\sigma_4(n_1+n_2)}$$

となる．この右辺は $\det(A_1)\det(A_4)$ に等しい．

5. 両辺とも $n(n-1)/2$ 次の式で，$a_i=a_j(i\neq j)$ のとき0となる．しかも $a_1^{n-1}\cdot a_2^{n-2}\cdots a_{n-1}\cdot 1$ の係数が一致する．

6. $a_1,a_2,\cdots,a_n$ が $\boldsymbol{C}$ 上の変数だとして，上式を示す．第1行から第 n 行をすべて加えると，$a_1+a_2+\cdots+a_n$ ができるから，左辺は $a_1+a_2+\cdots+a_n$ で割り切れる．また $\zeta^n=1$ のとき，左辺で，$a_1\longmapsto a_1$, $a_2\longmapsto\zeta a_2,\cdots,a_n\longmapsto\zeta^{n-1}a_n$ なるおき換えをしても行列式の値は変らない．よって左辺は右辺で割り切れる．そこで両辺とも $a_1,a_2,\cdots,a_n$ の同次式であることに注意して a_1^n の係数を比較すると，両辺が等しいことがわかる．

第 II 章

1. G を $X=G/H$ の上に，$G\times X\ni(g,aH)\longmapsto gaH\in X$ で作用させ，これによる G の置換表現を ρ とする．G は X 上に推移的に働き，ρ の核を N とすると，$N=\{g\in G \mid gaH=aH\ (\forall a\in G)\}=\bigcap_{a\in G}aHa^{-1}\subset H$ となる．ところが $X=G/H$ は有限集合だから，X 上の置換群 $S(X)$ も有限群であり，$[G:N]\leqq \sharp S(X)<\infty$ となる．

2. 巡回群 G/Z の生成元を aZ $(a\in G)$ とすると，G の任意の2元は $g_1=a^{n_1}z_1$, $g_2=a^{n_2}z_2$ $(n_1,n_2\in \boldsymbol{Z},\ z_1,z_2\in Z)$ と書ける．したがって，$g_1g_2=(a^{n_1}z_1)(a^{n_2}z_2)=a^{n_1}(z_1a^{n_2})z_2=a^{n_1}(a^{n_2}z_1)z_2=a^{n_1+n_2}z_1z_2=a^{n_2}(a^{n_1}z_2)z_1=a^{n_2}(z_2a^{n_1}z_1)=(a^{n_2}z_2)(a^{n_1}z_1)=g_2g_1$.

3. $G\neq\{1\}$ を p 群とすると，類等式より G の中心 Z は $\{1\}$ ではない（定理 8.22 の証明参照）．

（1） $\sharp G=p^2$ なら $\sharp Z=p$ または p^2 である．もし $\sharp Z=p$ なら，G/Z は位数 p の巡回群で，**2** より G もアーベル群となり矛盾する．$\sharp Z=p^2$ なら $G=Z$ はアーベル群である．

（2） $\sharp G=p^3$ かつ G がアーベル群でないとすると，**2** より $\sharp Z=p$, $G/Z\simeq \boldsymbol{Z}/p\boldsymbol{Z}\times\boldsymbol{Z}/p\boldsymbol{Z}$ となる．

4. シローの定理より，G の位数 g は素数 p のべき p^e で $e\leqq 3$ となるか，相異なる素数 p,q の積となる．$\boldsymbol{Z}/p\boldsymbol{Z}\times\boldsymbol{Z}/p\boldsymbol{Z}$ は3個以上の自明でない部分群をもつことに注意すると，**3** より $g=p^3$ なら，G はアーベル群で巡回群となることがわかる．$\boldsymbol{Z}/p^e\boldsymbol{Z}$ の自明でない部分群の個数は $e-1$ 個だから，この場合 $G\simeq\boldsymbol{Z}/p^3\boldsymbol{Z}$ のみが適する．$g=pq$ なら，G の p-シロー群 P も q-シロー群 Q も唯一つしかなく，とくに正規部分群となる．よって $G=P\times Q\simeq\boldsymbol{Z}/p\boldsymbol{Z}\times\boldsymbol{Z}/q\boldsymbol{Z}\simeq\boldsymbol{Z}/pq\boldsymbol{Z}$ となる．

5. $2275=5^2\times7\times13$ である．位数 2275 の群 G の 5-シロー群，7-シロー群，13-シロー群を各々 P_5,P_7,P_{13} で表すと，**3** よりすべてアーベル群となる．また 7-シロー群の個数を k_7 とすると，$k_7=[G:N_G(P_7)]$ は $[G:P_7]=5^2\cdot13$ の約数で，かつ $k_7\equiv1$ (7) となる．よって $k_7=1$ となり，$P_7\lhd G$ となる．同様にして，$P_{13}\lhd G$ となる．とくに P_7P_{13} は G の正規部分群となる．$H=P_7\cdot P_{13}$ の中で P_7,P_{13} は正規部分群で，

元の位数を考えることにより $P_7 \cap P_{13} = \{1\}$ となる．よって $H = P_7 \times P_{13}$ となり，$\sharp H = 7 \cdot 13$ となる．他方 $N_G(P_5) \supset P_5 \cdot H = G$ だから，$P_5 \triangleleft G$．よって，$P_5 \triangleleft G$, $H \triangleleft G$, $P_5 \cap H = \{1\}$ だから，$G = P_5 \times H$ はアーベル群となる．

6. $V = k^n$ を体 k 上の長さ n の縦ベクトル全体のなすベクトル空間とし，V の上に $G = GL(n, k)$ を行列の積により作用させる．V の k-ベクトル空間としての基底の全体を $\mathscr{V} = \{(v_1, v_2, \cdots, v_n)\}$ とおく．このとき G は $\mathscr{V}$ の上に，$g \cdot (v_1, v_2, \cdots, v_n) = (gv_1, gv_2, \cdots, gv_n)$ により作用し，この作用は忠実かつ推移的となる．よって $\sharp G = \sharp \mathscr{V}$ となるから，$\mathscr{V}$ の元の個数を数えればよい．

$v_1, v_2, \cdots, v_l \in V$ が張る V の k-部分空間を $\langle v_1, v_2, \cdots, v_l \rangle$ で表す．このとき，$(v_1, v_2, \cdots, v_n) \in \mathscr{V}$ となるためには，$\dim_k \langle v_1, v_2, \cdots, v_l \rangle = l$ $(1 \leqq l \leqq n)$ となることが必要かつ十分であり，そのためには $v_{l+1} \notin \langle v_1, v_2, \cdots, v_l \rangle$ $(1 \leqq l \leqq n-1)$ となることが必要かつ十分である．$\sharp V = q^n$ であるから，$v_1 \in V \setminus \{0\}$ のとり方は $q^n - 1$ 個ある．以下順に $v_1, v_2, \cdots, v_l$ をとったとき，v_{l+1} のとり方は $\sharp V - \sharp \langle v_1, v_2, \cdots, v_l \rangle = q^n - q^l$ 個ある．よって $\sharp G = \sharp \mathscr{V} = (q^n - 1)(q^n - q) \cdots (q^n - q^{n-1})$ である．

7. $\sigma \neq 1$ の互いに共通する文字を含まない巡回置換の積への表現を $\sigma = (i_1, i_2, \cdots, i_r) \cdots$ $(r > 1)$ とする．$r \geqq 3$ なら $\tau = (i_1, i_2)$ とおくと，$\sigma(i_1) = i_2 \neq i_3 = (\tau\sigma\tau^{-1})(i_1)$ となる．$r = 2$ なら $i_3 \notin \{i_1, i_2\}$ とし，$\tau = (i_1, i_3)$ とすると，$\sigma(i_2) = i_1 \neq i_3 = (\tau\sigma\tau^{-1})(i_2)$ となる．

8. G の部分群 H の指数を n とし，$G \times G/H \ni (g, aH) \longmapsto gaH \in G/H$ により G の G/H への作用を定める．これによる置換表現を ρ とすると，$G \neq H$ だから $\rho \neq 1$ である．もし G が単純群なら，$G \simeq \mathrm{Im}\,\rho \subset S(G/H) \simeq S_n$ となるが，$2 \leqq n \leqq 4$ だから S_n は可解群であり，その単純な部分群 G は，位数 2 または 3 の巡回群となる．

9. $\chi(g) \neq 1$ とし，$\chi(a) \neq 1$ とする．このとき

$$\textstyle\sum_{g \in G} \chi(g) = \sum_{g \in G} \chi(ag) = \chi(a) \sum_{g \in G} \chi(g)$$

だから，$\sum_{g \in G} \chi(g) = 0$ となる．

10. $\pi : G \longrightarrow G/Z$ を自然な準同型とする．$\pi(N) = \{1\}$ なら $N \subset Z$ であり，$N \cap Z \neq \{1\}$ である．$\pi(N) \neq \{1\}$ とする．べき零群 G の中心は $\{1\}$ ではないから，$\sharp G/Z < \sharp G$ である．よって G の位数に関する帰納法で，$n \in N$ で $\pi(n) \neq 1$ かつ $\pi(n)$ が G/Z の中心に入るものがとれる．$\pi(n) \neq 1$ だから $n \notin Z$ であり，$g \in G$ で $gn \neq ng$ なるものが存在する．このとき $\pi[n, g] = [\pi(n), \pi(g)] = 1$ だから，$[n,$

$g] = ngn^{-1}g \in Z$ である．よって $1 \neq n(gn^{-1}g) \in N \cap Z$ である．

11. $h_0 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ とおく．i が G の内部自己同型なら，$h_1 \in G$ があり，$i(g) = h_1 g h_1^{-1}$ $(\forall g \in G)$ となる．よって $h_0 g h_0^{-1} = h_1 g h_1^{-1}$ だから，$(h_0^{-1}h_1)g = g(h_0^{-1}h_1)$ $(\forall g \in G)$ となり，$h_0^{-1}h_1$ はスカラー行列 $\begin{pmatrix} \lambda & 0 \\ 0 & \lambda \end{pmatrix}$ $(\lambda \in \boldsymbol{R})$ となる．$-1 = \det(h_0^{-1}h_1) = \lambda^2 > 0$ だから，これは矛盾である．

12. S_4 の元の交換子 $[\sigma, \tau] = \sigma\tau\sigma^{-1}\tau^{-1}$ は偶置換だから A_4 に属す．よって交換子群 $D(S_4)$ は A_4 に含まれる．他方，

$$[(i\ l), (j\ l)] = (i\ l)(j\ l)(i\ l)(j\ l) = (i\ j\ l)$$

であるから，$D(S_4) \supset A_4$ である．よって問題のような χ があれば，$\mathrm{Ker}(\chi) \supset A_4$ となる．よって，$\chi(\sigma) = 1$ $(\forall \sigma \in S_4)$ か $\chi(\sigma) = \mathrm{sgn}(\sigma)$ となる．（$\Lambda = \mathrm{Inn}(G)$ とおき，$\mathrm{Ker}(\chi)$ が Λ-正規部分群であり，S_4 の Λ-正規部分群は S_4，A_4，クライン群 V，$\{1\}$ に限ることを示してもよい．）

13. 問題 6 と同様にすればよい．G は位数 p^3 の元 1 個と位数 p^2 の元 2 個で生成されている．G の位数 p^3 の元は，直積の第一成分への射影が $p\boldsymbol{Z}/p^3\boldsymbol{Z}$ に属さぬ．したがって，そのような元の p^2 倍として得られる元は，直積の第一成分が 0 ではない．そこで，G の中に最初に位数が p^3 の元をとり，次に位数 p^2 の元を 2 個独立にとる．このようなとり方の個数が，$\#(\mathrm{Aut}(G)) = (p^7 - p^6) \times (p^6 - p^4) \times (p^6 - p^5)$ である．

14. $\boldsymbol{Q} \ni a_1 = p_1/q_1$，$a_2 = p_2/q_2$，$p_1, p_2, q_1, q_2 \in \boldsymbol{Z}$，$(p_1, q_1) = 1$，$(p_2, q_2) = 1$ とする．このとき，$(p_2 q_1)a_1 = p_1 p_2 = (p_1 q_2)a_2$ となる．$\boldsymbol{Q} = A_1 \oplus A_2$，$A_1 \ni a_1 \neq 0$，$A_2 \ni a_2 \neq 0$ とすると，$\langle a_1 \rangle \cap \langle a_2 \rangle \subset A_1 \cap A_2 = \{0\}$ となるが，これは上のことに矛盾する．よって $\boldsymbol{Q}$ は直既約である．

これに対し，分母が素数 p のべきである有理数の全体を $\boldsymbol{Q}_{(p)}$ とおくと，$\boldsymbol{Q}/\boldsymbol{Z}$ は $\boldsymbol{Q}_{(p)}/\boldsymbol{Z}$ の p についての直和となる．

15. H は G の指数 2 の部分群であり，位数 2 の元を持たないから $|H|$ は奇数である．$G \ni a$，$H \not\ni a$ なる元をとる．$H \ni h$ とすると，$ha \in Ha$ の位数は 2 だから，$haha = 1$ となる．よって $h^{-1} = aha = aha^{-1}$ となる．そこで $h_1, h_2 \in H$ とすると，

$$h_1 h_2 = a(h_1 h_2)^{-1}a^{-1} = (ah_2^{-1}a^{-1})(ah_1^{-1}a^{-1}) = h_2 h_1$$

となり，H は奇数位数のアーベル群となる．このような G の例としては，n が奇数のときの 2 面体群 D_n がある．

第 Ⅲ 章

1.　$c \in C,\ a \in D,\ a \neq 0,\ -1$　とし，$c_1 = a^{-1}ca,\ c_2 = (a+1)^{-1}c(a+1)$ とおくと，$a(c_2 - c_1) = c - c_2$ が成り立つ．このとき，$c_1 \neq c \Longleftrightarrow c_2 \neq c$　が成り立ち，さらに上式より $c_2 \neq c_1$ とも同値となる．よって $ac \neq ca$ なら $c_2 - c_1 \neq 0$ となり，$a = (c - c_2)(c_2 - c_1)^{-1} \in C$　となる．

C が D の中心に含まれないものとし，$c \in C$ と $a_0 \in D$ で $a_0 c \neq c a_0$ なるものをとる．もし $a \in D,\ a \neq 0,\ -1$ が $ac \neq ca$ を満たすなら，上の議論により，$a \in C$ となる．$a = 0,\ -1$ なら $a \in C$ は明らかである．さらに，$ac = ca$ なら　$(a - a_0)c \neq c(a - a_0)$　であるから，$a_0, a - a_0 \in C$ となる．よって　$a = a_0 + (a - a_0) \in C$ となり，$C = D$ となる．

2.　$\boldsymbol{Q}$ の部分環を R とし，R の元 $a = m/n$ $(m, n \in \boldsymbol{Z},\ n \neq 0,\ (m, n) = 1)$ の分母 n の素因数分解 $n = p_1^{e_1} p_2^{e_2} \cdots p_t^{e_t}$ に現れる素数の全体を P とする．$(m, n) = 1$ だから $sm + tn = 1$ $(s, t \in \boldsymbol{Z})$ とすると，$R \ni sa + t = (sm + tn)/n = 1/n$　となる．よって　$R \ni p_1^{e_1 - 1} p_2^{e_2} \cdots p_t^{e_t}(sa + t) = 1/p_1$　となる．よって $p \in P$ なら $1/p \in R$ となる．これより容易に，$R = \{m/n \mid m \in \boldsymbol{Z},\ n = p_1^{e_1} p_2^{e_2} \cdots p_t^{e_t}(p_i \in P)\}$　と書けることがわかる．

3.　$f(x) = g(x)h(x),\ \ g(x) = b_0 + b_1 x + \cdots + b_m x^m,\ \ h(x) = c_0 + c_1 x + \cdots + c_l x^l$ と $R[x]$ 内で書けたとする．$a_0 = b_0 c_0$ はちょうど p で割り切れるから，b_0, c_0 のうち一方が p で割れ，他方は p では割れない．$p \mid b_0, p \nmid c_0$ とし，($p \nmid a_n$ に注意して) $b_0, b_1, \cdots, b_i$ は p で割り切れ，b_{i+1} は p では割り切れないとする．このとき，

$$a_{i+1} = (b_0 c_{i+1} + b_1 c_i + \cdots + b_i c_1) + b_{i+1} c_0$$

は p では割り切れない．よって $i + 1 = n$ となり，$m + l = n$ より $l = 0$ となる．よって $h(x) = b_0 \in R$ となり，$f(x)$ は原始的だから，$h(x) = b_0 \in U(R) = U(R[x])$　となる．

4.　(1)　共に既約である．

(2)　$g(x) \mid f(x)$　なら　$l = \deg g(x) \leqq \deg f(x)$　である．$l = 0, 1, 2, \cdots,\ l \leqq (\deg f(x))/2$ について，$f(0), f(1), \cdots, f(l)$ を計算し，その約数として，$g(0), g(1),$

$\cdots, g(l)$ が取り得る可能性を調べる．そこでこれらの組に対し，$g(x)$ を第Ⅰ章末，問題2の方法で作り，$f(x)$ が $g(x)$ で割り切れるかどうかを調べればよい．これはクロネッカーにより発見された方法である．

5.　$\mathfrak{a}=(x^2-yz)$ とおく．このとき $C[x,y,z]/\mathfrak{a}$ の代表元として，

$$f(x,y,z)=f_0(y,z)+f_1(y,z)x \qquad (f_i(y,z)\in C[y,z])$$

の形の多項式がとれる．このとき

$$(g_0(y,z)+g_1(y,z)x)(h_0(y,z)+h_1(y,z)x)\equiv g_0(y,z)h_0(y,z)$$
$$+(g_0(y,z)h_1(y,z)+g_1(y,z)h_0(y,z))x+g_1(y,z)h_1(y,z)yz \qquad (\mathrm{mod}\ \mathfrak{a})$$

であるから，x,y,z が素元であることはすぐわかる．

6.　（1）　$\mathfrak{a}=(\alpha_1,\alpha_2,\cdots,\alpha_r)$ とすると，環の準同型

$$R[y_1,y_2,\cdots,y_r]\ni g(y_1,y_2,\cdots,y_r) \longmapsto g(\alpha_1x,\alpha_2x,\cdots,\alpha_rx)\in S$$

は全射となる．定理 5.1 を使う．

（2）　$\mathfrak{a}^i\cap\mathfrak{b}\supset\mathfrak{a}^{i-k}(\mathfrak{a}^k\cap\mathfrak{b})$ は明らかである．問題の係数を比較することにより，$b\in\mathfrak{a}^{i-k}(\mathfrak{a}^k\cap\mathfrak{b})$ がわかるから，逆の包含関係が導かれる．

7.　（1）　$\mathfrak{b}=(b_1,b_2,\cdots,b_r)$ とすると，$a_{ij}\in\mathfrak{a}$ で，

$$a_{11}b_1+a_{12}b_2+\cdots+a_{1r}b_r=b_1$$
$$a_{21}b_1+a_{22}b_2+\cdots+a_{2r}b_r=b_2$$
$$\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots$$
$$a_{r1}b_1+a_{r2}b_2+\cdots+a_{rr}b_r=b_r$$

なるものが存在する．これは $b_1,b_2,\cdots,b_r$ についての，連立斉次1次方程式系だから，係数のなす行列式

$$d=\begin{vmatrix}1-a_{11} & -a_{12} & \cdots & -a_{1r}\\ -a_{21} & 1-a_{22} & \cdots & -a_{2r}\\ \cdots & \cdots & \cdots & \cdots\\ -a_{r1} & -a_{r2} & \cdots & 1-a_{rr}\end{vmatrix}\equiv 1 \qquad (\mathrm{mod}\ \mathfrak{a})$$

は，$db_i=0$ $(i=1,2,\cdots,r)$ を満たす（Ⅰ，系 10.7 参照）．よって，$d=1-a$ とおくと，$a\in\mathfrak{a}$ かつ $(1-a)\mathfrak{b}=0$ となる．

（2）　問題6，（b）より，$\mathfrak{a}^{k+1}\cap\mathfrak{a}^*=\mathfrak{a}(\mathfrak{a}^k\cap\mathfrak{a}^*)$ となる．よって $\mathfrak{a}^*\subset\mathfrak{a}\cdot\mathfrak{a}^*$ となる．したがって $\mathfrak{a}^*=\mathfrak{a}\cdot\mathfrak{a}^*$ が成り立つから，（a）より $\mathfrak{a}^*\subset\{x\in R\mid\exists a\in\mathfrak{a},\ ax=x\}$ となる．逆に $x\in R$ が，$\exists\, a\in\mathfrak{a},\ ax=x$ となるなら，$x=a^ix\in\mathfrak{a}^i$

$(\forall i \geqq 1)$ となり，$x \in \mathfrak{a}^*$ となる．

（3） $x \in R$, $a \in \mathfrak{m}$ が $ax = x$ を満たすなら，$1 - a$ は R の単数だから，$x = 0$ となる．

8. R が $\boldsymbol{C}$ 上有限個の元 $\{f_i(x, y)\}_{i=1}^m$ で生成されたとする．このとき $\{f_i(x, y) - f(0, 0)\}_{i=1}^m$ も R を生成するから，$f(0, 0) = 0$ とし，$f_i(x, y) = xg_i(x, y)$ $(g_i(x, y) \in \boldsymbol{C}[x, y])$ の形であるとしてよい．そうすると，

$$\boldsymbol{C}[xg_1, xg_2, \cdots, xg_m] = \{\sum c_{i_1 i_2 \cdots i_m}(xg_1)^{i_1}(xg_2)^{i_2}\cdots(xg_m)^{i_m}\}$$

となり，とくに $x\boldsymbol{C}[y]$ との交りは $\boldsymbol{C}xg_1 + \boldsymbol{C}xg_2 + \cdots + \boldsymbol{C}xg_m$ に含まれ，高々有限次元の $\boldsymbol{C}$ ベクトル空間となる．これは $x\boldsymbol{C}[y]$ が無限次元の $\boldsymbol{C}$ ベクトル空間であるということに矛盾する．なお $\boldsymbol{Z}[x]$ の部分環 $\boldsymbol{Z} + 2\boldsymbol{Z}[x]$ が有限生成でないことも同様にして証明できる．

9. Chinese Remainder Theorem (命題 1.8) を使い，ヒントのような b をとればよい．

10. $\mathfrak{p}_1 = (yz + 1) \subset k[y, z]$ とおく．ヒントのように展開するとき，

$$f(x, y, z) \equiv f_0(y, z) \qquad (\mathrm{mod}\ \mathfrak{p})$$

が成り立つ．ところが $k[x, y, z]/\mathfrak{p} \simeq k[y, z]/\mathfrak{p}_1 \simeq k[y, y^{-1}]$ は整域だから，$\mathfrak{p}$ と $\mathfrak{p}_1$ は素イデアルである．また

$$f(x, y, z) \equiv f_0(y, z) + f_1(y, z)x \qquad (\mathrm{mod}\ \mathfrak{q})$$

であるから，f の適当なべきが $\mathfrak{q}$ に属するためには，$f_0 \in \mathfrak{p}_1$ となることが必要かつ十分で，しかもこのとき $f^2 \in \mathfrak{q}$ となる．よって $\sqrt{\mathfrak{q}} = \mathfrak{p}$ で，

$$f, g \in \mathfrak{q}, \quad f \notin \mathfrak{p} \implies g \in \mathfrak{p}$$

が成り立つ．

11. 仮定より $d/g(x) = a(x)(f(x)/g(x)) + b(x)$ は無限個の整数で整数値をとる．ところが，d の約数の全体は有限個だから，$g(x)$ は無限個の点で同じ値をとる．よって $g(x)$ は定数である．

12. $\boldsymbol{Z}[x]$ の素元は，定理 4.8 の証明より，$\boldsymbol{Z}$ の素元である素数と，既約な原始多項式の 2 通りがある．

（1） $\mathfrak{p} \ni h(x)$ の素元分解を $h(x) = P_1^{e_1}P_2^{e_2}\cdots P_t^{e_t}$ とすると，$\mathfrak{p}$ は素イデアルだからある P_i が $\mathfrak{p}$ に属す．$\mathfrak{p} \cap \boldsymbol{Z} = \{0\}$ だから，この $P_i = f(x)$ は原始的既約多項式である．$\mathfrak{p}$ が $f(x)$ で割り切れない元を含むとする．$\mathfrak{p}$ は素イデアルだから，この元は $\boldsymbol{Z}[x]$ の素元だとしてよい．ところが $\mathfrak{p} \cap \boldsymbol{Z} = \{0\}$ だから，この元は $f(x)$ 以外の原

始的既約多項式 $g(x)$ となる．よって $\boldsymbol{Q}[x]$ で $a^*(x)f(x)+b^*(x)g(x)=1$ と書き，この分母を払って $a(x)f(x)+b(x)g(x)=d$ と書くと，$0\neq d\in\mathfrak{p}$ となり矛盾する．

（2）$\mathfrak{p}\cap\boldsymbol{Z}=(p)$（$p$ は素数）と書く．$\boldsymbol{Z}[x]/p\boldsymbol{Z}[x]\simeq(\boldsymbol{Z}/p\boldsymbol{Z})[x]$ は単項イデアル環だから，$\mathfrak{p}/p\boldsymbol{Z}[x]$ は $\{0\}$ でなければ，ある多項式 $f(x)$ の類で生成される．$\mathfrak{p}$ は素イデアルだから，この $f(x)$ は原始的既約多項式だとしてよい．

13. 略．

14. t に関する帰納法で，$a\in R$，$a\notin\mathfrak{p}_i$ $(i=1,2,\cdots,t)$ なるものが存在することを示す．

第 IV 章

1. 準同型定理 $N_1/N_1\cap N_2\simeq(N_1+N_2)/N_2$ を使う．

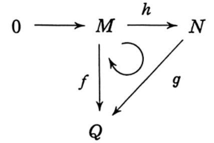
2. D を斜体，M を左 D–加群とする．M の部分集合で，D 上1次独立なもの全体を考え，包含関係により順序集合とする．ツォルンの補題を使い極大元 U をとれば，U は M を生成し，U は M の基底となる．逆にすべての左 D–加群が D–自由加群となるとする．$\mathfrak{l}$ を D の極大左イデアルとすれば，$D/\mathfrak{l}$ は既約で，かつ仮定より D–自由加群となる．よって $D/\mathfrak{l}\simeq D$ となり，D は左 D–加群として既約となる．よって D の左イデアルは D と $\{0\}$ に限るから，第III章，命題 1.1 より D は斜体となる．

3. 第II章，命題 5.4,（1）と問題 1.2 および問題 2.7 より，$m=p^e, n=q^f$ $(p,q$ 素数，$e,f\in\boldsymbol{N})$ の場合に求めればよい．この場合には，容易に次の結果を得る．

$$(\boldsymbol{Z}/p^e\boldsymbol{Z})\otimes_{\boldsymbol{Z}}(\boldsymbol{Z}/q^f\boldsymbol{Z})\simeq\begin{cases}0 & (p\neq q)\\ \boldsymbol{Z}/p^{\min(e,f)}\boldsymbol{Z} & (p=q),\end{cases}$$

$$\mathrm{Hom}_{\boldsymbol{Z}}(\boldsymbol{Z}/p^e\boldsymbol{Z},\boldsymbol{Z}/q^f\boldsymbol{Z})\simeq\begin{cases}0 & (p\neq q)\\ \boldsymbol{Z}/p^{\min(e,f)}\boldsymbol{Z} & (p=q).\end{cases}$$

4. ねじれ加群となるのは $\boldsymbol{Q}/\boldsymbol{Z}$ と $\boldsymbol{Z}/p\boldsymbol{Z}$，加除加群となるのは $\boldsymbol{Q}$ と $\boldsymbol{Q}/\boldsymbol{Z}$，射影的なものはなし，入射的なのは $\boldsymbol{Q}$ と $\boldsymbol{Q}/\boldsymbol{Z}$，平坦なのは $\boldsymbol{Q}$ のみ．



5. 命題 3.4,（2）を示す．単射な準同型 $h: M\to N$

と準同型 $f : M \longrightarrow Q$ が与えられたとする．$M \subset N$ で，h は自然なうめ込みだと仮定してよい．$M \subset L \subset N$ なる N の R-部分加群 L と，$g : L \longrightarrow Q$ なる準同型の組で，$(f|_L) = g\circ(h|_L)$ なる条件を満たす組 (L, g) の全体を考える．これは帰納的順序集合をなし，極大元 (L, g) が存在する．もし $L \subsetneqq N$ なら，$N \diagdown L \ni u$ をとり，$\mathfrak{l} = \{a \in R \mid au \in L\}$ を考える．$\mathfrak{l}$ は R の左イデアルで，$\varphi(a) = g(au)$ とおくと，$\varphi : \mathfrak{l} \longrightarrow Q$ なる準同型が定まる．仮定より，φ は $\tilde{\varphi} : R \longrightarrow Q$ なる準同型に拡張できる．L と u で生成される N の R-部分加群を L' とおき，L' の元 $l' = l + ru$ $(l \in L, r \in R)$ に対して $g'(l') = g(l) + \tilde{\varphi}(r)$ とおけば，$g' : L' \longrightarrow Q$ なる準同型は，$(f|_{L'}) = g'\circ(h|_{L'})$ を満たす．これは (L, g) の極大性に矛盾する．

6. (1) $m \in \mathrm{Ker}(\prod i_{\mathfrak{m}}) = \bigcap \mathrm{Ker}(i_{\mathfrak{m}})$ とする．このとき，$\mathfrak{a} = \{a \in R \mid am = 0\}$ は R のイデアルで，$\mathfrak{a}_{\mathfrak{m}} = \{a/s \in R_{\mathfrak{m}} \mid (a/s)(1 \otimes m) = 0\}$ を局所化としてもつ（命題 2.8，問題 2.9 参照）．ところが仮定より，$1 \otimes m = 0$ となるから $\mathfrak{a}_{\mathfrak{m}} = R_{\mathfrak{m}}$ となり，とくに $\mathfrak{a} \not\subset \mathfrak{m}$ $(\forall \mathfrak{m} \in \mathscr{M})$ である．よって $\mathfrak{a} = R \ni 1$ となり，$m = 0$ となる．

(2) $K = \mathrm{Ker}(f)$，$C = \mathrm{Coker}(f) = N/\mathrm{Im}(f)$ とおく．このとき，下の可換図式ができる．上の列は定義より完全だから，命題 2.8 より，下の列も完全となる．ところが縦の列は (1) より単射だから，すべての $K_{\mathfrak{m}}$ が $\{0\}$ なら K も $\{0\}$ となり，すべての $C_{\mathfrak{m}}$ が $\{0\}$ なら C も $\{0\}$ となる．よって十分性がでた．必要性は明らかである．

$$
\begin{array}{ccccccccc}
0 & \longrightarrow & K & \longrightarrow & M & \longrightarrow & N & \longrightarrow & C & \longrightarrow 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \downarrow & \\
0 & \longrightarrow & \prod_{\mathfrak{m}} K_{\mathfrak{m}} & \longrightarrow & \prod_{\mathfrak{m}} M_{\mathfrak{m}} & \longrightarrow & \prod_{\mathfrak{m}} N_{\mathfrak{m}} & \longrightarrow & \prod_{\mathfrak{m}} C_{\mathfrak{m}} & \longrightarrow 0
\end{array}
$$

7. (1) $\pi : M \longrightarrow M/\mathfrak{a}M$，$\pi' : M' \longrightarrow M'/\mathfrak{a}M'$ を自然な準同型とし，$\bar{f} : M/\mathfrak{a}M \longrightarrow M'/\mathfrak{a}M'$ を左 $R/\mathfrak{a}$-加群としての同型とする．
M は射影的で，π' は全射だから，準同型 $f : M \longrightarrow M'$ で右図を可換とするものが存在する．ここで $\mathfrak{a} \subset J(R)$ だから，中山の補題より，$M' = f(M)$ が成り立つ．ところが M' は射影的だから，準同型

$$
\begin{array}{ccc}
M & \xrightarrow{\ \pi\ } & M/\mathfrak{a}M \\
{\scriptstyle f}\downarrow & \circlearrowleft & \downarrow{\scriptstyle \bar{f}} \\
M' & \xrightarrow[\ \pi'\ ]{} & M'/\mathfrak{a}M'
\end{array}
$$

$g : M' \longrightarrow M$ で $f\circ g = \mathrm{id}_{M'}$ となるものが存在する．この g は単射であり，$\pi\circ g = (\bar{f})^{-1}\circ(\bar{f}\circ\pi)\circ g = (\bar{f})^{-1}\circ(\pi'\circ f)\circ g = (\bar{f})^{-1}\circ\pi'$ となる．よって中山の補題より，$M = g(M')$ が成り立つ．よって g は同型である．

（2）Rを局所環，$\mathfrak{m}$をRの極大イデアル，Mを有限生成な射影的R-加群とする．$R/\mathfrak{m}$は体だから，階数が有限なR-自由加群Fで，$M/\mathfrak{m}M$と$F/\mathfrak{m}M$が$R/\mathfrak{m}$-加群として同型となるものが存在する．よって（1）より，$M \simeq F$となる．

8.　（1）$\Longrightarrow$（2）．A_iをヒントのとうりとすると，$i>0$, $n>j\geqq 0$のとき，

$$\longrightarrow \mathrm{Ext}_R^i(P_j, N) \longrightarrow \mathrm{Ext}_R^i(A_{j+1}, N) \longrightarrow \mathrm{Ext}_R^{i+1}(A_j, N) \longrightarrow \mathrm{Ext}_R^{i+1}(P_j, N) \longrightarrow$$

が完全となる．ところがP_jは射影的だから，$\mathrm{Ext}_R^i(P_j, N)=0$, $\mathrm{Ext}_R^{i+1}(P_j, N)=0$となり，$\mathrm{Ext}_R^i(A_{j+1}, N) \simeq \mathrm{Ext}_R^{i+1}(A_j, N)$となる．よって

$$\mathrm{Ext}_R^1(P_n, N) = \mathrm{Ext}_R^1(A_n, N) = \cdots = \mathrm{Ext}_R^{n+1}(A_0, N) = \mathrm{Ext}_R^{n+1}(M, N) = 0$$

となる．したがって，$0 \longrightarrow M_1 \longrightarrow M_2 \longrightarrow P_n \longrightarrow 0$が左$R$-加群の完全列なら，Extの完全列より，

$$0 \longrightarrow \mathrm{Hom}_R(M_1, N) \longrightarrow \mathrm{Hom}_R(M_2, N) \longrightarrow \mathrm{Hom}_R(P_n, N) \longrightarrow 0$$

も完全となる．

（2）$\Longrightarrow$（3）．Mの射影的分解　$\cdots \longrightarrow P_n \longrightarrow P_{n-1} \longrightarrow \cdots \longrightarrow P_0 \longrightarrow M \longrightarrow 0$　を1つとり，P_nを$\mathrm{Ker}(P_{n-1} \longrightarrow P_{n-2})$でおき換えればよい．

（3）$\Longrightarrow$（1）．（3）の射影的分解より，$\mathrm{Ext}_R^{n+1}(M, N)$を計算する．

9.　（1）KをMの商体とする．Mが平坦なら，うめ込み$R \hookrightarrow K$より作った$M \longrightarrow K\otimes M$が単射となる．ところがこの写像の核は，$\{m\in M \mid 1\otimes m=0\} = \{m \in M \mid rm=0\ (0\neq \exists r\in R)\} = t(M)$　だから，Mのねじれ元は0に限る．逆にMが0以外のねじれ元をもたないものとする．$M=\bigcup_{i\in I} M_i$と，Mを有限生成なR-部分加群の和の形に表す．このとき，各M_iは有限生成なR-加群で，ねじれ元は0に限るから，R-自由加群となり，平坦である．$f: N_1 \longrightarrow N_2$を$R$-加群の単射とする．このとき，$\mathrm{Ker}(\mathrm{id}_M \otimes f) = \mathrm{Ker}(M\otimes_R N_1 \longrightarrow M\otimes_R N_2) = \bigcup_{i\in I} \mathrm{Ker}(M_i\otimes N_1 \longrightarrow M_i \otimes N_2) = 0$である．よって$M$は平坦である．

（2）問題5とその逆を使う．Mが入射的だとし，$0\neq a\in R$, $m\in M$について，$f_m: Ra \ni ra \longmapsto rm \in M$　を考える．これが$f: R\longrightarrow M$に拡張されるから，$m=f_m(1)=f(a)=af(1)\in aM$　となり，Mは可除加群となる．逆にMが可除可群で，RaをRのイデアル，$g: Ra \longrightarrow M$をR-加群の準同型とする．$g(1)=m\in M$を$m=am'$ $(m'\in M)$と書き，$g': R\ni r \longmapsto rm' \in M$とおくと，これは$g$の$R$への拡張となる．

10.　（1）$e_1^{-1}qe_1 = \xi_0e_0+\xi_1e_1-\xi_2e_2-\xi_3e_3$, $e_2^{-1}qe_2=\xi_0e_0-\xi_1e_1+\xi_2e_2-\xi_3e_3$,

$e_3^{-1}qe_3=\xi_0e_0-\xi_1e_1-\xi_2e_2+\xi_3e_3$　である．

（2）　$q=e_1^{-1}qe_1=e_2^{-1}qe_2=e_3^{-1}qe_3$　なら，（1）より $\xi_1=\xi_2=\xi_3=0$ となる．また $\mathfrak{a}$ を A の両側イデアルで，$\mathfrak{a}\ni q=\xi_0e_0+\xi_1e_1+\xi_2e_2+\xi_3e_3\neq 0$ とする．このとき（1）より，$\mathfrak{a}\ni\xi_0e_0,\xi_1e_1,\xi_2e_2,\xi_3e_3$　となる．ところが $e_0=1$，$e_1^2=\alpha$，$e_2^2=\beta$，$e_3^2=-\alpha\beta$　だから，$\mathfrak{a}\ni\xi_0$，$\alpha\xi_1$，$\beta\xi_2$，$-\alpha\beta\xi_3$　となる．よって，K は体だから，$\mathfrak{a}\ni 1$ となり，A は単純環となる．

（3）　定理 6.12 より，K を含む斜体 D で，$A\simeq M_n(D)$ となるものが存在する．この式の両辺の K 上の次元を調べると，$4=\dim_K A=n^2\dim_K D$ となる．よって $n^2\leqq 4$ だから，$n=1$ で $A=D$ となるか，$n=2$ で $A=M_2(K)$ となる．ところが K は体だから，

$$N(q)=q\bar{q}\neq 0 \iff q(\bar{q}N(q)^{-1})=1 \iff q\ \text{は逆元をもつ}$$

が成り立つ．よって，「$q\neq 0$ なら $N(q)\neq 0$」が成り立つなら $A=D$ となり，そうでないなら $A\simeq M_2(K)$ となる．

第 V 章

1.　R を有限整域，$a\in R, a\neq 0$ とする．R は整域だから，$m_a: R\ni x\longmapsto ax\in R$ は単射である．よって $\#m_a(R)=\#(R)$ となり，m_a は全射となる．

2.　$\text{trans.deg}_K M\leqq\text{trans.deg}_K L$ であり，この右辺は定理 9.1 より有限である．よって，M/K の超越基底を $y_1,y_2,\cdots,y_s$ とし，$K'=K(y_1,y_2,\cdots,y_s)$ とおくと，K'/K は有限生成で，M/K' は代数的である．

L/K' の超越基底を $x_1,x_2,\cdots,x_r$ とすると，M/K' は代数的だから，(問題 9.2 より) これらは M 上でも代数的に独立である．よって，$m_1,m_2,\cdots,m_d\in M$ が K' 上 1 次独立なら，これらは $K'(x_1,x_2,\cdots,x_r)$ 上でも 1 次独立となる．ところが，L は $K'(x_1,x_2,\cdots,x_r)$ 上有限生成な代数拡大だから，有限次拡大となる．よって　$[M:K']\leqq[L:K'(x_1,x_2,\cdots,x_d)]<\infty$　だから，M/K' は有限生成となる．よって M/K は有限生成である．

3.　$f_i(x)$ の根を α_i とすると，α_i は $f(x)$ の根だから，$\bar{K}/K$ の K-同型 σ_i で，$\sigma_i(\alpha_1)=\alpha_i$ となるものが存在する．このとき，L/K は正規だから，$L[x]/(f_1(x))\simeq L(\alpha_1)$

$\simeq L^{\sigma_i}(\alpha_i) = L(\alpha_i) \simeq L[x]/(f_i(x))$ となる．とくに，α_i の $f_i(x)$ での重複度は i にはよらない．よって，$e_i = (\alpha_i$ の $f(x)$ での重複度$)/(\alpha_i$ の $f_i(x)$ での重複度) も i のとり方にはよらない．

4. (1) $K^{p^{-\infty}}$ の元はすべて K 上純非分離的だから，$\mathrm{Aut}(\bar{K}/K)$ の元で動かない．よって $F(\mathrm{Aut}(\bar{K}/K)) \supset K^{p^{-\infty}}$ である．逆に $\theta \in F(\mathrm{Aut}(\bar{K}/K))$ とすると，問題2.12より，θ の K 上の共役元は θ に限る．よって，θ は K 上純非分離的であり，$K^{p^{-\infty}}$ に属す．

(2) M が完全体なら，純非分離的方程式 $x^{p^e} - a = 0$ $(a \in K)$ の根 $a^{p^{-e}}$ は M に属す．よって $M \supset K^{p^{-\infty}}$ である．逆に $M \supset K^{p^{-\infty}}$ とする．(1) より $K^{p^{-\infty}} = F(\mathrm{Aut}(\bar{K}/K))$ と書けるから，定理5.1,(1) より，$\bar{K}/K^{p^{-\infty}}$ はガロア拡大となり，とくに分離的である．よって $\bar{K}/M$ も分離的である．

(3) (2) より $[K^{p^{-\infty}} : K] = 1$ または ∞ を示せばよいから，この次元が有限だとし，$K^{p^{-\infty}} = K$ を示す．$K^{p^{-e}} = \{\theta \in \bar{K} \mid \theta^{p^e} \in K\}$ とおくと，$K^{p^{-\infty}} = \bigcup_{1 \leq e < \infty} K^{p^{-e}}$ である．仮定より，ある e につき $K^{p^{-e}} = K^{p^{-(e+1)}}$ が成り立つ．この両辺の p^{e-1} 乗をとると，$K = K^{p^{-1}}$ となり，$K = K^{p^{-1}} = K^{p^{-2}} = \cdots = K^{p^{-e}} = \cdots = K^{p^{-\infty}}$ となる．

5. L/L_s は純非分離拡大，L_s/K は分離拡大だから，$[L : K]_s = [L_s : K]$ が成り立つ．また，L_s/K は有限次分離拡大だから単拡大である．よって，定理4.9より，$L_s = K$ の場合に同値性を示せばよい．

$L = K(\theta)$ で $\theta^{p^e} \in K$, $\theta^{p^{e-1}} \notin K$ なら，$L^{p^e} \subset K$, $L^{p^{e-1}} \not\subset K$, $[L : K] = p^e$ が成り立つ．逆に $L^{p^e} \subset K$, $L^{p^{e-1}} \not\subset K$, $[L : K] = p^e$ が成り立つなら，$\theta \in L$ で $\theta^{p^e} \in K$, $\theta^{p^{e-1}} \notin K$ なるものをとると，$L \supset K(\theta) \supset K$, $[L : K] = p^e = [K(\theta) : K]$ が成り立つ．よって $L = K(\theta)$ となる．

6. (1),(2) は易しいので省略する．

(3) $D_p = \langle \sigma, \tau \mid \sigma^p = \tau^2 = 1,\ \tau^{-1}\sigma\tau = \sigma^{-1} \rangle$ の部分群は，D_p と $\{1\}$ の他，位数 p のものは $\langle \sigma \rangle$，位数2のものは $\langle \sigma^{-i}\tau\sigma^i \rangle$ $(i = 0, 1, 2, \cdots, p-1)$ がある．対応する部分体は，$K = C(x^p + x^{-p})$，$L = C(x)$，$C(x^p)$，$C((\xi^{-i}x) + (\xi^{-i}x)^{-1})$ である．

7. M/K はガロア拡大で，そのガロア群は

$$\bar{\sigma}:\ \sqrt{2} \longmapsto -\sqrt{2},\ \sqrt{3} \longmapsto \sqrt{3}$$
$$\bar{\tau}:\ \sqrt{2} \longmapsto \sqrt{2},\ \sqrt{3} \longmapsto -\sqrt{3}$$

で生成される．ところが $\theta^2 = -(2+\sqrt{2})(3+\sqrt{6}) \in M$ だから，

$$\bar{\sigma}(\theta^2) = -(2-\sqrt{2})(3-\sqrt{6}) = (\sqrt{2}-1)^2(\sqrt{3}-\sqrt{2})^2\theta^2,$$
$$\bar{\tau}(\theta^2) = -(2+\sqrt{2})(3-\sqrt{6}) = (\sqrt{3}-\sqrt{2})^2\theta^2$$

が成り立つ．よって　$\sigma(\theta) = (\sqrt{2}-1)(\sqrt{3}-\sqrt{2})\theta \in L$, $\tau(\theta) = (\sqrt{3}-\sqrt{2})\theta \in L$　だから，$\sigma, \tau \in \mathrm{Aut}(L/K)$　となる．

$\langle\sigma\rangle$ による不変体は $\boldsymbol{Q}(\sqrt{3})$，$\langle\tau\rangle$ による不変体は $\boldsymbol{Q}(\sqrt{2})$ だから，$G = \langle\sigma, \tau\rangle$ による不変体は $\boldsymbol{Q} = K$ となる．よって L/K はガロア拡大である．$\sigma^4 = \tau^4 = 1$，$\sigma\tau = \tau^3\sigma$ なることは，σ, τ の定義式より容易に確かめられる．

8. （1）　直接計算により，容易にわかる．

（2）　右辺の体が対応する群で不変なことはすぐわかる．そこで，上のものから順に，$\boldsymbol{Q}$ 上の次数を調べればよい．

（3）　$1+\zeta+\zeta^2+\cdots+\zeta^{15}+\zeta^{16}=1$　に注意して，ζ の式に展開すればよい．

9. （1）　$F(x)$ を $y_1, y_2, \cdots, y_n, x$　の多項式とみたとき，その係数は $\alpha_1, \alpha_2, \cdots, \alpha_n$ の $\boldsymbol{Z}$-係数の多項式で，S_n の元による置換で不変である．よって，例 5.8 の後の注により，$\alpha_1, \alpha_2, \cdots, \alpha_n$ の基本対称式の $\boldsymbol{Z}$-係数の多項式となる．よって $F(x)$ の係数は，$f(x)$ の係数の $\boldsymbol{Z}$-係数多項式で書けるから，R に入る．

（2）　$\alpha_1 y_{\sigma(1)} + \alpha_2 y_{\sigma(2)} + \cdots + \alpha_n y_{\sigma(n)} = \alpha_{\sigma^{-1}(1)} y_1 + \alpha_{\sigma^{-1}(2)} y_2 + \cdots + \alpha_{\sigma^{-1}(n)} y_n$ $(\forall\sigma \in S_n)$ が成り立つ．しかも

$$\mathrm{Aut}(\bar{K}(y_1, y_2, \cdots, y_n)/K(y_1, y_2, \cdots, y_n)) \simeq \mathrm{Aut}(\bar{K}/K)$$

だから，$\sigma \in G_f$ なら，この元と　$\alpha_1 y_1 + \alpha_2 y_2 + \cdots + \alpha_n y_n$　は $K(y_1, y_2, \cdots, y_n)$ 上共役である．よって $\sigma(F_1(x)) = F_1(x)$ となる．逆に $\sigma(F_1(x)) = F_1(x)$ なら $\sigma \in G_f$ となるから，（2）が成り立つ．

（3）　$F(x) = F_1(x)F_2(x)\cdots F_r(x)$　を（2）のとうりとする．$F(x)$ は一意分解環 $R[y_1, y_2, \cdots, y_n]$ に係数をもつ多項式だから，第Ⅲ章，系 4.11 より，$F_i(x) \in R[y_1, y_2, \cdots, y_n][x]$ としてよい．そこで上式の係数の $(\bmod\ \mathfrak{p})$ をとったものを，$\tilde{F}(x) = \tilde{F}_1(x)\tilde{F}_2(x)\cdots\tilde{F}_r(x)$　とする．この $\tilde{F}(x)$ は，$\tilde{f}(x) \in \tilde{K}[x]$ より（1）の手続きにより作られたものともみなせる．そこで　$\tilde{F}_1(x) \in \tilde{K}[y_1, y_2, \cdots, y_n][x]$ を素因数分解し，$x - (\tilde{\alpha}_1 y_1 + \tilde{\alpha}_2 y_2 + \cdots + \tilde{\alpha}_n y_n)$ を含む因子を $\tilde{F}_{11}(x)$ とおく．$\tilde{F}_{11}(x)$ は $\tilde{F}_1(x)$ の因子で，$\tilde{F}_{11}(x)$ をそれ自身に移す $\sigma \in S_n$ の全体が，$\tilde{f}(x)$ の $\tilde{K}$ 上のガロア群 $G_{\tilde{f}}$ をなす．もし $\sigma \in S_n$ が $F_1(x)$ を $F_i(x)$ $(i \neq 1)$ に移すなら，σ は $\tilde{F}_1(x)$ を $\tilde{F}_i(x)$ に移す．ところが $\tilde{F}(x)$ は分離的だから，$\sigma(\tilde{F}_{11}(x)) \neq \tilde{F}_{11}(x)$ となる．よって $G_{\tilde{f}}$

$\subset G_f$ となる.

10. 有限体の有限次拡大は巡回拡大だから，方程式 $f(x)=0$ の K 上のガロア群は巡回群である．そこで σ をその生成元とすると，$\langle\sigma\rangle$ は各 $f_i(x)$ の根の集合の上に推移的に作用する．よって σ の型は，問題のようになる．

11. $f(x)=x^5-x-1$ は $(\mathrm{mod}\ 2)$ では $(x^2+x+1)(x^3+x^2+1)$ と素因数分解される．よって問題 9,（3）と問題 10 より，G_f は，$(i\ j)(k\ l\ m)$ 型の置換を含む．これは 3 乗すると互換となるから，根の番号をつけ替え，$(1\ 2)\in G_f$ としてよい．また $f(x)$ は $(\mathrm{mod}\ 3)$ では既約だから，G_f は 5 次の巡回置換 ρ を含む．$\langle\rho\rangle$ は $\{1,2,\cdots,5\}$ の上に推移的に作用するから，適当なべきは $(1\,2\,p\,q\,r)$ の形となる．そこで番号をつけ替え，$(1\ 2\ 3\ 4\ 5)\in G_f$ とする．このとき，$(1\ 2),(2\ 3),\cdots,(4\ 5)\in G_f$ となるから，第 II 章，問題 3.6 より，$G_f=S_5$ となる．後半は，n 次多項式 $g(x)\in \boldsymbol{Z}[x]$ で，$(\mathrm{mod}\ 2)$ では（2 次式）×（1 次式）× ⋯ ×（1 次式）と分解され，$(\mathrm{mod}\ 3)$ では既約となるものを，Chinese Remainder Theorem（III，命題 1.8,（2））を使って作り，その分解体をとればよい．

12. （1） L/M は定理 8.1,（2）の形である．仮定より，$\sigma(a)\in M$ だから，$\sigma^{l^m}(\sigma(a))=\sigma(a)$ となる．よって $\sigma^{l^m}(\sigma(\sqrt[l]{a}))=\zeta^i\sigma(\sqrt[l]{a})$ $(1\leqq i<l)$ と書けるから，$\sigma^{l^m}(\sigma(\sqrt[l]{a})/(\sqrt[l]{a})^i)=\sigma(\sqrt[l]{a})/(\sqrt[l]{a})^i$ となる．あとは簡単な計算でわかる．

（2） $N_{M/K}(b^l)=\zeta^l=1$ だから，系 7.7 より，このような $a\in M$ が存在する．τ の $\bar{K}/K$ の同型への拡張を $\bar{\sigma}$ で表すと，a のとり方より，$\bar{\sigma}(\sqrt[l]{a})/\sqrt[l]{a}=\zeta^i b\,(0\leqq i<l)$ と書ける．よって $\bar{\sigma}(\sqrt[l]{a})\in L$ だから，L/K はガロア拡大となる．$\bar{\sigma}$ の L への制限を σ と表すと，$\sigma^{l^m}(\sqrt[l]{a})=N_{M/K}(\zeta^i b)\sqrt[l]{a}=\zeta\sqrt[l]{a}$ となる．よって，$\sigma^{l^m}\neq 1$, $\sigma^{l^{m+1}}=1$, $F(\langle\sigma\rangle)=K$ となり，$\mathrm{Gal}(L/K)=\langle\sigma\rangle\simeq \boldsymbol{Z}/l^{m+1}\boldsymbol{Z}$ となる．

（3） $\boldsymbol{Q}(\sqrt{-d})\ni\theta=\alpha+\beta\sqrt{-d}$ $(\alpha,\beta\in\boldsymbol{Q})$ のノルムは，$\alpha^2+d\beta^2\geqq 0$ となり，$N_{\boldsymbol{Q}(\sqrt{-d})/\boldsymbol{Q}}(\theta)=-1$ は解がない．$l=2$ として（1）を使う．

13. （1） θ が根なら，$\theta+1,\theta+2,\cdots,\theta+p-1$ も根である．$\sigma\longmapsto\sigma(\theta)-\theta$ なる対応により，$\mathrm{Gal}(L/K)\simeq\boldsymbol{Z}/p\boldsymbol{Z}$ となる．

（2） $H^1(\mathrm{Gal}(L/K),L)=0$ だから，ヒントが成り立つ（問題 7.8 参照）．K は標数 p の体だから，$Tr_{L/K}(1_K)=p1_K=0$ となり，$1=\sigma(\beta)-\beta$ $(\beta\in L)$ と書ける．$\sigma(\beta)=\beta+1$ だから，$\sigma(\beta)^p-\sigma(\beta)=\beta^p-\beta$ は K に属す．よって β は，$f(x)=x^p-x-(\beta^p-\beta)\in K[x]$ の根である．

14. (1) (a) $\boldsymbol{Q}(\sqrt{2})/\boldsymbol{Q}$ はガロア拡大で，そのガロア群は id と $\rho:\sqrt{2}\longmapsto -\sqrt{2}$ が作る位数 2 の群．(b) $\boldsymbol{Q}(\sqrt{3},\sqrt{5})$ が求める体で，そのガロア群は，$\sqrt{3}\longmapsto\pm\sqrt{3}, \sqrt{5}\longmapsto\pm\sqrt{5}$ が作る位数 4 の群，$\simeq(\boldsymbol{Z}/2\boldsymbol{Z})\times(\boldsymbol{Z}/2\boldsymbol{Z})$．(c) $\boldsymbol{Q}(\sqrt{-1},\sqrt[4]{8})$ が求める体で，ガロア群は，$\sqrt{-1}\longmapsto\pm\sqrt{-1}$，$\sqrt[4]{8}\longmapsto(\sqrt{-1})^i\sqrt[4]{8}$ $(i=0,1,2,3)$ が作る位数 8 の 2 面体群．(d) 自明なものの他，$\boldsymbol{Q}(\sqrt{3}),\boldsymbol{Q}(\sqrt{5}),(\boldsymbol{Q}(\sqrt{15})$ の計 5 個 (e) 自明なものの他，2 次体 $\boldsymbol{Q}(\sqrt{-1})$，$\boldsymbol{Q}(\sqrt{2}),\boldsymbol{Q}(\sqrt{-2})$，4 次体 $\boldsymbol{Q}((\sqrt{-1})^i\sqrt[4]{8})$ $(i=0,1,2,3)$ の計 9 個．(f) ガロア閉包は $\boldsymbol{Q}(\sqrt{-3},\sqrt[3]{5},\sqrt[3]{7},\sqrt[3]{11})$ で，そのガロア群 G は，分解型完全列

$$1\longrightarrow(\boldsymbol{Z}/3\boldsymbol{Z})^3\longrightarrow G\longrightarrow U(\boldsymbol{Z}/3\boldsymbol{Z})\longrightarrow 1$$

を満たす．$\boldsymbol{Q}(\sqrt[3]{5},\sqrt[3]{7},\sqrt[3]{11})/\boldsymbol{Q}$ の中間体は，G の $U(\boldsymbol{Z}/3\boldsymbol{Z})$ を含む部分群と 1 対 1 に対応し，さらに $\boldsymbol{Q}(\sqrt{-3})$ との合成体をとることにより，$(\boldsymbol{Z}/3\boldsymbol{Z})^3$ の部分群と 1 対 1 に対応する．ところが，第 II 章末の問題 6 の証明より，このような $(\boldsymbol{Z}/3\boldsymbol{Z})^3$ の部分群の個数は，位数が 3 のものが $(3^3-1)/(3-1)=13$ 個，位数が 3^2 のものが $(3^3-1)(3^3-3)/(3^2-1)(3^2-3)=13$ 個 である．よって求める個数は $2+13+13=28$ 個 である．

あとがき

この本の執筆においては，執筆方針等の点から，主に服部〔B 1〕と永尾〔B 2〕を参考にさせて戴いた．また部分的には，佐武〔D 1〕や，浅野，永尾〔E 1〕，彌永，小平〔B 4〕，ファン・デル・ベルデン〔B 7〕，数学辞典〔A 1〕等も参考にさせて戴いた．

本書は，〔B 1〕に比べて説明を詳しくし，〔B 2〕に比べて内容を多くしたつもりである．

参考文献

[A] 数学全般について

〔A 1〕 数学辞典(第三版)，岩波書店，1985

〔A 2〕 ブルバキ：数学原論，東京図書

[B] 代数学全般について

〔B 1〕 服部 昭：現代代数学，朝倉書店，1968

非常によく書けているが，簡潔すぎて，初心者には読みにくいかも知れない．

〔B 2〕 永尾 汎：代数学，朝倉書店，1983

良書だが，他の部分に比べ，群論に関する部分が詳しい．

〔B 3〕 阿部英一：代数学，培風館，1977

これも良書だが，ページ数に比べ，内容が多い．

〔B 4〕 彌永昌吉，小平邦彦：現代数学概説 I，岩波書店，1961

集合とホモロジーを参考にした．

〔B 5〕 彌永昌吉，布川正巳：代数学，岩波書店，1968

単因子の理論を参考にした．

〔B 6〕 ブルバキ：数学原論，代数 1-7，東京図書，1968-1970

標準的教科書であり，非常に詳しい．しかし教科書としては量が多すぎる．

〔B 7〕 ファン・デル・ベルデン：現代代数学 1-3，東京図書，1959-60

古典的名著であり，読みやすい．体論と単因子の理論を参考にした．

〔B 8〕 正田建二郎：抽象代数学，岩波書店，1932

古典的名著である．

〔B 9〕 堀田良之：代数入門—群と加群，裳華房，1987

この本の4章までと，本書のⅣ章までとは，大体同じ方針で書かれている．

〔B 10〕 S. Lang：Algebra，Addison-Wesley，1965

アメリカでの標準的教科書である．

〔B 11〕 N. Jacobson：Lectures in abstract algebra，Ⅰ，Ⅱ，Ⅲ，Van Nostrand，1951-1964，Springer GTM 30, 31, 32，1976

体論の部分（Vol. Ⅲ）が詳しくてよい．

〔B 12〕 永田雅宜：代数学講話，現代数学社，1983

これは大学院数学入試問題より適当なものを集めたものであり，章末の問題を作成するのに参考にした．

［C］ 集合と位相について

〔C 1〕 加藤十吉：集合と位相，朝倉書店，1982

〔C 2〕 内田伏一：集合と位相，裳華房，1986

200ページと短いにもかかわらず，必要な事項が良くまとまっている．

〔C 3〕 河田敬義，三村征雄：現代数学概説 Ⅱ，岩波書店，1965

〔C 4〕 ブルバキ：数学原論，集合論 1-3，東京図書，1968-1969

〔C 5〕 ブルバキ：数学原論，位相 1-5，東京図書，1968

［D］ 線型代数について

〔D 1〕 佐武一郎：線型代数学，裳華房，1974

線型代数についての名著である．行列式の部分を参考にした．

［E］ 群について

〔E 1〕 浅野啓三，永尾 汎：群論，岩波書店，1965

読みやすい．指標の理論等を参考にした．

〔E 2〕 鈴木通夫：群論 上，下，岩波書店，1977-78

〔E 3〕 近藤 武：群論(基礎数学講座)，岩波書店，1976-77

〔E 4〕 M. Hall：Theory of groups，Macmillan，1959

〔E 5〕 D. Gorenstein：Finite groups, Harper & Row, 1968

[**F**] 環について

〔F 1〕 松村英之：可換環論，共立出版，1980

〔F 2〕 永田雅宜：可換環論，紀伊国屋書店，1974

〔F 3〕 ブルバキ：数学原論，可換代数 1-4，東京図書，1971-1972

〔F 4〕 M. Nagata：Local rings, Interscience, 1962

〔F 5〕 O. Zariski and P. Samuel：Comutative algebra Ⅰ，Ⅱ，Van Nostrand, 1958-1960, Springer GTM. 28, 29, 1976

〔F 6〕 C. W. Curtis and I. Reiner：Representation theory of finite groups and associative algebra, Interscience, 1962

群の表現と関係した非可換環に詳しい．

〔F 7〕 N. Jacobson：Theory of rings, Amer. Math. Soc. Surveys, 1943

半単純環の標準的教科書である．

〔F 8〕 N. Jacobson：Structure of rings, Amer. Math. Soc. Colloq. Publ. 1956

[**G**] ホモロジー代数について

〔G 1〕 H. Cartan and S. Eilenberg：Homological algebra, Princeton Univ. Press, 1956

ホモロジーについての古典的名著である．

〔G 2〕 R. Godement：Topologie algébrique et théorie des faisceux, Hermann, 1958

層の理論に関したホモロジーに詳しい．名著である．

〔G 3〕 S. MacLane：Homology, Springer, 1963

[**H**] 体論について

〔H 1〕 永田雅宜：可換体論（新版），裳華房，1985

体についての名著である．

索　　引

記　　号

事　　項

ア

イ

ウ

エ　オ

カ

ス

セ

ソ

タ

ナ

ニ

ネ　ノ

ハ

ヒ

フ

ヘ

ホ

ミ

ム モ

ヤ

人　名

著者略歴

1945 年　和歌山県生まれ．

1970 年　東京大学理学系研究科修士課程修了，同年，東京大学理学部助手．その後，北海道大学理学部講師，助教授，東北大学理学部助教授を経て，1988 年より，東北大学理学部教授．この間，プリンストン高等研究所（1972－74），ボン大学（1977－78），ボルドー大学（1982），ゲッチンゲン大学（1987）等の客員研究員．理学博士．

数学選書 9．**代　数　概　論**

1987 年 11 月 20 日　第 1 版発行©
2001 年 3 月 30 日　第11版発行

検印省略

定価はカバーに表示してあります．

著作者　森田康夫（もりたやすお）

発行者　吉野達治

発行所　東京都千代田区四番町 8 番地
電話　東京　3262-9166～9
株式会社　裳華房

印刷所　横山印刷株式会社

製本所　株式会社　青木製本所

社団法人
自然科学書協会会員

ISBN 4-7853-1311-0

Printed in Japan